Journées mathématiques X-UPS

Année 2000

Groupes finis

Anne-Marie Aubert

Un peu d'histoire des groupes finis et quelques exemples simples

Journées mathématiques X-UPS (2000), p. 1-56.
https://doi.org/10.5802/xups.2000-01

Les Éditions de l'École polytechnique
Route de Saclay
F-91128 PALAISEAU CEDEX
https://www.editions.polytechnique.fr

Centre de mathématiques Laurent Schwartz
CMLS, École polytechnique, CNRS,
Institut polytechnique de Paris
F-91128 PALAISEAU CEDEX
https://portail.polytechnique.edu/cmls/

Publication membre du
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org

Journées mathématiques X-UPS
2000, p. 1–56 doi: 10.5802/xups.2000-01

UN PEU D'HISTOIRE DES GROUPES FINIS ET QUELQUES EXEMPLES SIMPLES

par

Anne-Marie Aubert

Table des matières

Publication originelle dans Journées X-UPS 2000. Groupes finis. Éditions de l'École polytechnique, 2000.

1. Introduction

Un angle d'approche de la théorie des groupes finis est fournie par l'analogie entre cette théorie et la théorie des nombres élémentaire. Afin d'illustrer cette analogie, considérons la division des entiers naturels. On dit qu'un entier naturel m divise un entier naturel n s'il existe un entier naturel q tel que $n = mq$. On dit alors que q est le quotient de n par m. Les entiers naturels les plus simples de ce point de vue sont les nombres $p \neq 1$ dont les seuls diviseurs sont 1 et p lui-même : on les appelle les nombres premiers. Un fait central est le résultat suivant : tout entier naturel $n \neq 1$ s'écrit $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ pour des nombres premiers distincts $p_1, p_2, \ldots, p_k$ et des entiers naturels $e_1, e_2, \ldots, e_k$, où chaque couple (p_i, e_i) est uniquement déterminé à permutation des indices près. Afin de mieux montrer l'analogie en vue, nous énonçons ce fait sous la forme équivalente suivante : pour tout entier naturel $n \neq 1$ il existe une suite $n = n_0 \geqslant n_1 \geqslant n_2 \geqslant \cdots \geqslant n_{r-1} \geqslant n_r = 1$ telle que chaque n_i/n_{i+1} est premier, et la suite de nombres premiers ainsi obtenue et ses multiplicités sont uniquement déterminée par n à l'ordre près. Il n'y a clairement pas unicité des entiers n_i eux-mêmes. Ce résultat est fondamental car il montre que les nombres premiers ne sont pas seulement simples du point de vue de la divisibilité mais qu'ils sont aussi les blocs fondamentaux permettant d'obtenir tout entier naturel par multiplications de nombres premiers.

Quelle est l'analogie avec la théorie des groupes finis ? L'analogue de la divisibilité est constitué par la notion de « distinction » : si H est un sous-groupe d'un groupe fini G, le quotient G/H de G par H est formé des classes à gauche de H dans G. Celles-ci sont précisément les classes d'équivalence pour la relation de congruence modulo H, définie par $g \equiv g' \pmod{H}$ si $g^{-1}g' \in H$. Le quotient G/H est un groupe pour loi de multiplication des classes $gHg'H = gg'H$ si et seulement si H est *distingué* (ou *normal*) dans G, *i.e.,* si $gH = Hg$ pour tout élément de g de G.

Exemple. Prenons pour G le groupe symétrique $\mathfrak{S}_n$ des permutations d'un ensemble à n éléments et pour H l'ensemble $\mathfrak{A}_n$ des permutations paires qui est un sous-groupe normal de G tel que $G/H \simeq Z_2$, le groupe cyclique à 2 éléments.

Quel est, dans ce contexte, l'analogue d'un nombre premier ? Un groupe G dont les seuls sous-groupes distingués sont $\{1\}$ et G lui-même (où 1 désigne l'élément neutre de G). Un tel groupe G est appelé un groupe *simple*.

Quel est l'analogue du résultat arithmétique énoncé ci-dessus ? Nous devons ici nous restreindre aux groupes finis, le théorème suivant n'étant pas vrai pour un groupe infini arbitraire. Traduisant le résultat sous la seconde forme évoquée ci-dessus, nous obtenons le *théorème de Jordan-Hölder*[(1)] *pour les groupes finis* : étant donné un groupe fini G, il existe une suite

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{r-2} \supset G_{r-1} \supset G_r = \{1\}$$

de sous-groupes G_i de G telle que le sous-groupe G_{i+1} est distingué dans G_i et G_i/G_{i+1} est un groupe simple pour tout $i \in \{0, 1, \ldots, r\}$ et la famille de groupes simples ainsi obtenue est unique à permutation près. Une telle suite est appelée une *suite de composition* de G.

Cette analogie présente toutefois quelques imperfections : par exemple, chacun des n_i divise n, alors que G_i n'est pas nécessairement distingué dans G, et l'on peut se demander si les groupes simples constituent les « blocs fondamentaux » des groupes finis.

Supposons que nous connaissions tous les groupes finis simples. Comment pourrions nous alors déterminer tous les groupes finis ? Tout d'abord, nous aimerions écrire une liste $S_1, S_2, \ldots, S_r$ de facteurs de composition simples. Nous essayerions alors de dresser une liste de tous les groupes G_i possibles tels que $G_i/G_{i+1} \simeq S_{i+1}$. La première étape est facile : puisque $G_r = \{1\}$, nous obtenons $G_{r-1} = G_{r-1}/G_r = S_r$. La deuxième étape consisterait à à déterminer, connaissant $G_{r-2}/G_{r-1} \simeq S_{r-1}$ et G_{r-1}, les possibilités pour G_{r-2}. C'est un exemple du *problème d'extension de Hölder*, qui

(1) Otto Ludwig Hölder s'est intéressé à la théorie des groupes à cause des travaux de Kronecker et de Klein. Il démontra l'unicité à permutation près des facteurs de composition dans une suite de composition d'un groupe fini. En 1892, en utilisant les théorèmes de Sylow, il montra que tous les groupes finis simples d'ordre inférieur à 200 étaient connus. Il étudia aussi les groupes d'ordre p^3, pq^2, pqr et p^4 pour p, q, r premiers. Il introduisit les notions d'automorphisme intérieur et extérieur, et écrivit en 1895 un long article sur les extensions de groupes.

peut s'énoncer sous la forme générale suivante : étant donnés deux groupes K et Q, déterminer tous les groupes G possibles tels que K est distingué dans G et $G/K \simeq Q$. De tels groupes G sont appelés des *extensions* de K par Q. Remarquons que si un groupe simple G est une extension de K par Q, alors $G \simeq K$ ou bien $G \simeq Q$. Le groupe n'est pas uniquement déterminé par la donnée de K et de Q : par exemple, les groupes $\mathfrak{S}_3$ et Z_6 (le groupe cyclique d'ordre 6) sont tous deux extensions de Z_3 par Z_2. La question est : toutes les extensions possibles G peuvent-elles être construites de manière systématique ? La réponse est oui, bien que peu économique. Schreier, dans les années vingt, a développé une technique pour construire toutes les tables de multiplication pour G, mais jusqu'à présent, à ma connaissance, il n'existe pas de méthode générale permettant d'identifier quelles tables de multiplication sont celles de groupes isomorphes (voir [Rot95, chap. 7] ou [Sco87, chap. 9] pour plus de détails). La liste des tables de multiplication possibles comprendrait donc des répétitions inutiles, néanmoins toutes les extensions G de K par Q peuvent être construites.

Maintenant que nous avons vu comment déterminer tous les groupes possibles G_{r-2}, nous pouvons continuer d'appliquer la méthode de Schreier afin de construire toutes les possibilités pour les groupes G_{r-3}, G_{r-4},... Les groupes finis simples apparaissent donc comme les blocs fondamentaux de la théorie des groupes finis.

2. Les groupes finis simples

Un exercice facile consiste à prouver que les groupes cycliques Z_p d'ordre premier p sont simples. Ce sont les seuls groupes finis simple abéliens. Évariste Galois avait essentiellement montré que les groupes alternés $\mathfrak{A}_n$, pour $n \geqslant 5$, constituent une famille infinie de groupes finis simples non abéliens (pour une preuve élémentaire de la simplicité on pourra se référer, par exemple, à [Jac75, Vol. I, p. 139]).

Les familles infinies suivantes de groupes finis simples furent découvertes parmi les *groupes classiques*, terminologie introduite par Hermann Weyl dans son livre [Wey39], publié en 1939. Ce sont les groupes de matrices qui furent introduits pour la première fois par

Camille Jordan [Jor89] et dont la structure fut étudiée de manière intensive par Leonard Dickson [Dic58, Dic01]. Dickson fut élève de Eliakim Moore à Chicago [Par89]. Son livre [Dic58] constitue non seulement la première étude systématique des groupes linéaires classiques mais il contient un travail profond et original sur ces groupes et les familles de groupes simples (pour une biographie de Dickson, voir [Par91]). Cependant ses méthodes étaient pour la plupart *ad hoc* et très calculatoires. Une approche plus élégante et plus lisible fut obtenue plusieurs années après grâce aux travaux d'Emil Artin [Art96, Art55b, Art55a], Jean Dieudonné [Die71], Bertram Huppert [Hup67, chap. 2] et Nathan Jacobson [Jac85].

La première famille de groupes classiques est la famille des *groupes linéaires généraux* $\mathrm{GL}(V)$ formés des automorphismes (*i.e.,* des transformations linéaires inversibles) d'un espace vectoriel V sur un corps commutatif k. Le groupe $\mathrm{GL}(V)$ est isomorphe au groupe $\mathrm{GL}_N(k)$ des matrices carrées d'ordre N inversibles à coefficients dans le corps k, où N est la dimension de V sur k. Les *groupes spéciaux linéaires* $\mathrm{SL}(V)$ (resp. $\mathrm{SL}_N(k)$) formés des automorphismes de V (resp. matrices carrées d'ordre N à coefficient dans k) de déterminant égal à 1. Le groupe $\mathrm{SL}_N(k)$ est égal au groupe des commutateurs[(2)] de $\mathrm{GL}_N(k)$, excepté dans le cas $N = 2$ et $k = \mathbb{F}_2$ (le corps à deux éléments).

Les autres groupes classiques sont les groupes d'automorphismes de formes non dégénérées sur V (espace vectoriel sur un corps commutatif k). Une *forme* sur V est une application $f\colon V \times V \to k$ telle que $f(v_1+v_2, v') = f(v_1, v')+f(v_2, v')$ et $f(v, v_1'+v_2') = f(v, v_1')+f(v, v_2')$ pour tous v, v_1, v_2, v', v_1', v_2' dans V. La forme f est *non dégénérée* si ses noyaux gauche et droit

$$\left\{v \in V \mid f(v, v') = 0 \ \text{ pour tout } v' \in V\right\},$$
$$\left\{v' \in V \mid f(v, v') = 0 \ \text{ pour tout } v \in V\right\}$$

---

(2)Le *groupe des commutateurs* $G' = [G, G]$ d'un groupe G est le sous-groupe de G engendré par les *commutateurs* $g_1 g_2 g_1^{-1} g_2^{-1}$ avec g_1, g_2 éléments de G. Si N est un sous-groupe distingué de G, le groupe quotient G/N est abélien si et seulement si N contient G'.

sont tous deux réduits à $\{0\}$. Le *groupe d'automorphismes* de la forme f est l'ensemble des automorphismes u de V qui préservent f au sens suivant : $f(uv, uv') = f(v, v')$ pour tout $(v, v') \in V \times V$.

Une forme F est *bilinéaire symétrique* si $f(v, v') = f(v', v)$ et $f(\lambda v, v') = \lambda f(v, v')$ pour tout $(v, v') \in V \times V$ et tout $\lambda \in k$. Le groupe d'automorphismes d'une telle forme est appelé un *groupe orthogonal* et sera noté $\mathrm{O}_N(k, f)$. Une forme f est *bilinéaire antisymétrique* si $f(v', v) = -f(v, v')$ et $f(\lambda v, v') = \lambda f(v, v')$ pour tout $(v, v') \in V \times V$ et tout $\lambda \in k$. Le groupe d'automorphismes d'une telle forme est appelé un *groupe symplectique* et sera noté $\mathrm{Sp}_N(k, f)$.

Si la caractéristique du corps k est égale à 2, les définitions ci-dessus des groupes orthogonaux et symplectiques coïncident. Les groupes usuellement appelés groupes orthogonaux doivent préserver une forme quadratique en sus de la forme bilinéaire symétrique. C'est pourquoi certains des énoncés ci-après concernant les groupes orthogonaux doivent être raffinés lorsque la caractéristique de k est 2 (pour plus de détails, on pourra se référer à [Che97, chap. 1]).

Les autres formes qui nous intéressent ici sont les formes sesquilinéaires hermitiennes. Ici k est une extension quadratique séparable d'un corps k_0 telle qu'il existe un automorphisme $\lambda \mapsto \overline{\lambda}$ de k sur k_0 d'ordre 2. Une forme f est *sesquilinéaire hermitienne* si $f(v', v) = \overline{f(v, v')}$ et $f(\lambda v, v') = \lambda f(v, v')$ pour tout $(v, v') \in V \times V$ et tout $\lambda \in k$. Le groupe d'automorphismes d'une telle forme est appelé un *groupe unitaire* et sera noté $\mathrm{U}_N(k, f)$.

Les groupes classiques restant (*i.e.,* autres que $\mathrm{GL}_n(k)$ et $\mathrm{SL}_n(k)$) sont les groupes d'automorphismes de formes non dégénérées de l'un des trois types ci-dessus.

Les formes antisymétriques sont non dégénérées seulement si N est pair [Art96]. Nous poserons alors $m := N/2$. D'autre part, deux formes non dégénérées antisymétriques sur V définissent des groupes symplectiques isomorphes. Nous écrirons donc simplement $\mathrm{Sp}_{2m}(k)$ pour $\mathrm{Sp}_{2m}(k, f)$. Les éléments de $\mathrm{Sp}_{2m}(k)$ ont leur déterminant égal à 1 et $\mathrm{Sp}_{2m}(k)$ coïncide avec son groupe des commutateurs, excepté lorsque $m = 1$ et k a deux ou trois éléments, et lorsque $m = 2$ et k a deux éléments. Lorsque k est fini, deux formes bilinéaires symétriques non dégénérées sur V définissent des groupes orthogonaux isomorphes lorsque N est impair (nous écrirons alors simplement $\mathrm{O}_N(k)$ pour $\mathrm{O}_N(k,f)$), et il y a exactement deux classes d'isomorphismes de groupes orthogonaux si N est pair, elles correspondent au cas où l'indice de Witt de la forme f est maximal ou non [Art96]. Nous écrirons $\mathrm{O}_N^+(k)$ et $\mathrm{O}_N^-(k)$ pour $\mathrm{O}_N(k,f)$ respectivement dans le premier et le second cas. Le groupe des commutateurs de $\mathrm{O}_N(k,f)$, noté $\Omega_N(k,f)$, est en général un sous-groupe propre du groupe de rotations $\mathrm{SO}_N(k,f)$ formé des éléments de $\mathrm{O}_N(k,f)$ de déterminant égal à 1. Toujours sous l'hypothèse k fini, deux formes sesquilinéaires hermitiennes non dégénérées sur V définissent des groupes unitaires isomorphes, et nous écrirons $\mathrm{U}_N(k)$ pour $\mathrm{U}_N(k,f)$. Lorsque $N \geqslant 3$, excepté le cas $N=3$ et $|k|=4$, le groupe des commutateurs de $\mathrm{U}_N(k)$ coïncide avec le sous-groupes $\mathrm{SU}_N(k)$ des éléments de $\mathrm{U}_N(k)$ de déterminant égal à 1. Lorsque $N=2$, le groupe $\mathrm{SU}_2(k)$ est isomorphe au groupe $\mathrm{SL}_2(k)$.

Il existe une procédure uniforme permettant d'associer un groupe simple à un groupe classique G arbitraire. On considère le groupe des commutateurs G' de G et l'on forme le groupe quotient $G'/\mathrm{Z}(G')$ de G' par son centre $\mathrm{Z}(G')$. Le groupe $\mathrm{Z}(G')$ est formé de multiples scalaires de l'identité et n'est pas un groupe compliqué. Lorsque k est fini, $\mathrm{Z}(G')$ est un sous-groupe du groupe multiplicatif (cyclique) de k. La plupart du temps, $G'/\mathrm{Z}(G')$ est un groupe simple [Art96], [Die71]. Il y a quelques exceptions en petites dimensions et sur de petits corps, et d'autres exceptions dans le cas unitaire lorsque la forme f est anisotrope(3). L'on obtient ainsi six familles de groupes dont les membres sont le plus souvent simples :

$$\begin{aligned}
\mathrm{PSL}_n(k) &:= \mathrm{SL}_n(k)/\,\mathrm{Centre},\\
\mathrm{PSp}_{2m}(k) &:= \mathrm{Sp}_{2m}(k)/\,\mathrm{Centre},\\
\mathrm{PSU}_n(K) &:= \mathrm{SU}_n(K)/\,\mathrm{Centre},
\end{aligned}$$

et trois familles de groupes orthogonaux

$$\Omega_{2m+1}(k)/\,\mathrm{Centre},\quad \Omega_{2m}^+(k)/\,\mathrm{Centre}\quad\text{et}\quad \Omega_{2m}^-(k)/\,\mathrm{Centre}\,.$$

(3) Une forme f est *anisotrope* si $f(v,v)\neq 0$ pour tout $v\neq 0$ dans V.

Lorsque k est fini, malgré quelques cas d'isomorphismes entre des groupes appartenant à des familles différentes, on obtient six familles doublement infinies.

Dickson découvrit aussi des familles de groupes simples associés aux algèbres de Lie simples de type G_2 et E_6 sur le corps $\mathbb{C}$ des nombres complexes dans trois articles [Dic02], [Dic05], [Dic07].

Jusqu'en 1955, on ne découvrit pas d'autre groupe fini simple excepté cinq groupes apparemment isolés qui avaient été découverts par Émile Mathieu en 1861 et 1873 [Mat61], [Mat73]. Avant de décrire les groupes de Mathieu, il est nécessaire d'introduire quelques éléments de terminologie des groupes de permutations. Une *représentation de permutation* d'un groupe fini G est un homomorphisme $\rho\colon G \to \mathfrak{S}(X)$ de G dans le groupe symétrique $\mathfrak{S}(X)$ des permutations d'un ensemble X. La représentation ρ est *fidèle* si son noyau est réduit à $\{1\}$, où 1 désigne l'élément neutre de G. L'image d'une représentation de permutation, ou sous-groupe quelconque de $\mathfrak{S}(X)$, est un *groupe de permutations* sur l'ensemble X. Si H est un groupe de permutation sur X, et x un élément de X, le *stabilisateur* H_x de x est l'ensemble $\{h \in H \mid hx = x\}$. Il est facile de vérifier que H_x est un sous-groupe de H. Étant donné un groupe de permutation H sur X, on définit une relation d'équivalence $\sim$ sur X par $x \sim x'$ s'il existe $h \in H$ tel que $x' = hx$. Les classes d'équivalence de $\sim$ sont les *orbites* de H sur X ou simplement les H-orbites. Si X est lui-même une H-orbite, on dit que H est un *groupe de permutations transitif.* Si x et x' appartiennent à une même H-orbite, leurs stabilisateurs H_x et $H_{x'}$ sont des sous-groupes conjugués de H. En particulier, tous les stabilisateurs sont conjugués lorsque H est un groupe de permutations transitif sur X. Un groupe de permutation G sur un ensemble X est dit *m-transitif* si tout m-uplet d'éléments distincts de X peut être envoyé sur n'importe quel m-uplet d'éléments distincts de X par une permutation appartenant à G. Un groupe est 1-transitif si et seulement s'il est transitif.

Exemples. Le groupe symétrique $\mathfrak{S}_n$ des permutations d'un ensemble à n éléments est m-transitif pour tout entier $m \leqslant n$. Le groupe alterné $\mathfrak{A}_n$ est m-transitif pour tout entier $m \leqslant n-2$. Les groupes symétriques $\mathfrak{S}_n$ (pour $n \geqslant 6$) et les groupes alternés $\mathfrak{A}_n$ (pour $n \geqslant 8$) sont les seuls groupes de permutations connus qui sont m-transitifs pour tout entier entier $m \geqslant 6$. Par ailleurs, il existe une infinité d'exemples de groupes de permutations 2-transitifs ou même 3-transitifs autres que les groupes symétriques et alternés. Les groupes d'automorphismes des géométries projectives sur les corps finis sont toujours 2-transitifs sur les points et, dans le cas des droites projectives, ils sont même 3-transitifs sur les points [Car56, chap. 12].

À côté des groupes symétriques et alternés, il y a seulement quatre groupes de permutations connus qui sont 4-transitifs ou 5-transitifs sur un ensemble fini. Ce sont les *groupes de Mathieu* découverts par Mathieu en 1861 et 1873. Le groupe de Mathieu M_{12} est un groupe d'ordre $95040 = 2^6 3^3 5 \cdot 11$ qui est 5-transitif sur un ensemble de cardinal 12. Le groupe de Mathieu M_{24} est un groupe d'ordre $244\,823\,040 = 2^{10} 3^3 5 \cdot 7 \cdot 11 \cdot 23$ qui est 5-transitif sur un ensemble de cardinal 24. Le stabilisateur d'un point quelconque dans M_{12} (resp. M_{24}) est le groupe de Mathieu M_{11} (resp. M_{23}) : c'est un groupe d'ordre $7920 = 2^4 3^5 5 \cdot 11$ (resp. $10\,200\,960 = 2^7 3^2 5 \cdot 7 \cdot 11 \cdot 23$) qui est 4-transitif sur un ensemble de cardinal 11 (resp. 23). Le stabilisateur d'un point quelconque dans M_{23} est le groupe de Mathieu M_{22} : c'est un groupe d'ordre $443\,520 = 2^7 3^5 5 \cdot 7 \cdot 11$. Les cinq groupes de Mathieu M_{11}, M_{12}, M_{22}, M_{23} et M_{24} sont simples et ne sont isomorphes ni à un groupe alterné ni à un groupe fini de type de Lie. Puisqu'ils ne figurent dans aucune famille infinie de groupes simples, William Burnside [Wag78], dans son livre [Bur55, Note N, p. 504], les appela *groupes simples sporadiques* et le terme *sporadique* est maintenant utilisé pour tout groupe fini simple qui n'appartient à aucune famille infinie de groupes simples.

Dans son célèbre article [Che55], Claude Chevalley développa une procédure de construction de familles infinies de groupes simples (appelés *groupes de Chevalley*) associés aux diverses *algèbres de Lie simples*(4) complexes de dimension finie. La classification des algèbres

(4)Une *algèbre de Lie* complexe L est une algèbre (un espace vectoriel muni d'un produit bilinéaire noté $[\,,\,]$) telle que les identités $[x,x] = 0$ et $[[x,y],z] +$

de Lie simples complexes de dimension finie, commencée par Wilhelm Killing, fut complétée en 1894 par Élie Cartan. Les groupes classiques sur $k = \mathbb{C}$ sont des *groupes de Lie* et leurs sous-groupes simples correspondent canoniquement aux algèbres de Lie simples complexes. Il y a donc plus qu'une analogie entre groupes simples et algèbres de Lie simples. Chevalley a montré que les familles infinies de groupes finis simples associées aux algèbres de Lie simples de type F_4, E_7 et E_8 étaient nouvelles. Des variations sur la méthode de Chevalley permirent à Robert Steinberg et Jacques Tits de construire de nouvelles familles infinies de groupes simples. Enfin Rimhak Ree montra qu'une famille construite de manière différente par Michio Suzuki [ABFS99] dans [Suz60] pouvait s'interpréter à l'aide d'un automorphisme du diagramme d'une algèbre de Lie de type B_2, et construisit des groupes analogues dans les cas G_2 et F_4, voir [Car89].

3. Groupes extra-spéciaux, groupes de Heisenberg, groupe métaplectique

Préliminaires

Groupe de Frattini [Ema89]. Soit G un groupe fini. Nous notons $\mathrm{Z}(G)$ et G' respectivement son centre et son groupe dérivé.

Définition 3.1. *Le* groupe de Frattini *d'un groupe fini G, noté $\Phi(G)$, est l'intersection des sous-groupes propres maximaux de G.*

Proposition 3.2. *Soient p un nombre premier et P un p-groupe fini (*i.e., *un groupe fini dont le cardinal est une puissance de p).*

(a) *Le groupe de Frattini de P est le plus petit des sous-groupes distingués H de P tels que le groupe quotient P/H soit abélien élémentaire.*

(b) *Le groupe $P/\Phi(P)$ a une structure naturelle d'espace vectoriel sur le corps $\mathbb{F}_p$ à p éléments. Cet espace vectoriel est appelé l'*espace

$[[y,z],x] + [[z,x],y] = 0$ sont satisfaites. Un idéal I de L est sous-espace vectoriel tel que $[x,I] \subset I$ pour tout $x \in L$. Une algèbre de Lie L est *simple* si $[L,L] \neq 0$ et si les seuls idéaux de L sont $\{0\}$ et L.

de Frattini *de P. La dimension de l'espace de Frattini est le nombre minimum de générateurs de P.*

(c) *Si P est d'exposant p, on a $\Phi(P) = P'$.*

Remarque. Si G est un groupe fini, alors G' est le plus petit des sous-groupes distingués H de G tels que G/H est abélien. Si P est un p-groupe, on a donc $P' \subset \Phi(P)$.

Un résultat sur les groupes de classe 2

Proposition 3.3. *Soit G un groupe de classe* 2*, (*i.e., *tel que $G' \subset \mathrm{Z}(G)$). Alors :*

(a) *pour tout élément g de G, l'application $x \mapsto [g, x]$ est un morphisme de groupes de G dans G' ;*

(b) *pour tout entier $k \geqslant 1$, et tout couple (g_1, g_2) d'éléments de G, on a*

$$(g_1 g_2)^k = [g_2, g_1]^{\Sigma(k)}\, g_1^k\, g_2^k, \quad \text{avec } \Sigma(k) := 1 + 2 + \cdots + (k-1).$$

Définition et exemples de groupes extra-spéciaux généralisés

Proposition 3.4

(a) *Le centre d'un p-groupe est non trivial.*

(b) *Tout groupe fini G qui possède un sous-groupe Z central (*i.e., *contenu dans $\mathrm{Z}(G)$) et tel que le quotient G/Z est cyclique, est abélien.*

Définition 3.5. *Un p-groupe est dit* extra-spécial généralisé *(respectivement* extra-spécial*) s'il possède un sous-groupe Z d'ordre p tel que $\Phi(E) \subset Z \subset \mathrm{Z}(E)$ (resp. si $\Phi(E)$ est d'ordre p et égal à $\mathrm{Z}(E)$).*

Proposition 3.6. *Tout p-groupe extra-spécial généralisé E est de l'un des types suivants :*

(a) *si E est abélien, il est*

- *abélien élémentaire (de type $(p, \ldots, p)$),*
- *ou du type $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$;*

(b) *si E est non abélien, alors son groupe de Frattini est central d'ordre p (et dans ce cas $Z = E' = \Phi(E)$).*

En particulier, tout p-groupe extra-spécial généralisé non abélien est de classe 2.

Remarque. Soit E un groupe d'ordre p^3 non abélien. Le centre $\mathrm{Z}(E)$ de E n'est pas trivial, et n'est pas d'indice p, donc est d'ordre p. Le quotient $E/\mathrm{Z}(E)$ n'est pas cyclique, donc est un groupe de type (p,p). Donc, $\mathrm{Z}(E)$ contient $\Phi(E)$. Comme ce dernier groupe n'est pas trivial, (sinon, E serait de type (p,p,p)), on voit que $\Phi(E) = \mathrm{Z}(E)$. Enfin, le groupe dérivé E' est contenu dans $\Phi(E)$ et n'est pas trivial, donc est égal à $\Phi(E)$.

Tout groupe non cyclique d'ordre p^3 est extra-spécial généralisé.

Rappelons qu'un sous-groupe d'un groupe fini G est dit *caractéristique* s'il est stable par toute automorphisme de G (en particulier, tout sous-groupe caractéristique de G est distingué dans G).

Si E est un p-groupe extra-spécial généralisé non abélien, le groupe de Frattini de E et le groupe dérivé de E sont cycliques et centraux dans E. Ceci nous amène à donner la définition suivante.

Définition 3.7. *Un* CC-groupe *est un groupe fini résoluble non abélien E dont tout sous-groupe caractéristique propre est cyclique et central dans E.*

Proposition 3.8. *Le groupe dérivé E' d'un CC-groupe est d'ordre premier p et E/E' est abélien p-élémentaire.*

Les CC-groupes apparaissent comme un cas particulier des groupes du type suivant. Soit E un groupe fini non abélien possédant un sous-groupe central Z d'ordre p, pour lequel on suppose choisi une fois pour toutes un isomorphisme avec le groupe additif de $\mathbb{Z}/p\mathbb{Z}$.

Si le groupe E/Z est abélien élémentaire, ce groupe est muni d'une structure naturelle d'espace vectoriel sur $\mathbb{F}_p$; on note V cet espace vectoriel. Un tel groupe E est appelé une *extension centrale* de V par $\mathbb{Z}/p\mathbb{Z}$. On a alors $1 \neq E' \subset \Phi(E) \subset Z$. Donc, $E' = \Phi(E) = Z$, et E est un groupe extra-spécial généralisé non abélien. En particulier, un CC-groupe est un p-groupe extra-spécial généralisé non abélien.

Réciproquement, soit E un p-groupe extra-spécial généralisé non abélien. De la relation $E' = \Phi(E)$, il résulte que E/E' est un p-groupe abélien élémentaire : c'est donc un espace vectoriel sur $\mathbb{F}_p$, que l'on note V et dont la loi est notée additivement. On a la suite exacte

$$1 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow E \longrightarrow V \longrightarrow 1.$$

Puisque $E' \subset \mathrm{Z}(E)$, le groupe E est de classe 2.

Structure des groupes extra-spéciaux généralisés

Soit E un p-groupe extra-spécial généralisé non abélien. Soit z un élément qui engendre E', choisi une fois pour toutes. Soit ζ l'application $\zeta\colon E' \to \mathbb{F}_p$ définie par $\zeta(z) := 1$. En d'autres termes, on a $\zeta([x,y]) = \alpha$, si $[x,y] = z^\alpha$.

Proposition 3.9. *Soit E un p-groupe extra-spécial généralisé non abélien.*

(a) *L'application $E \times E \to \mathbb{F}_p$*

$$(x,y) \longmapsto \zeta([x,y])$$

induit par passage au quotient une forme bilinéaire $a_E\colon V \times V \to \mathbb{F}_p$, qui est alternée.

(b)

- *Si $p \neq 2$, l'application $E \to \mathbb{F}_p$*

$$x \longmapsto \zeta(x^p)$$

induit par passage au quotient une forme linéaire $f_E\colon V \to \mathbb{F}_p$. Alors G est d'exposant p si et seulement si f_E est la forme nulle.

- *Si $p = 2$, l'application $E \to \mathbb{F}_2$*

$$x \longmapsto \zeta(x^2)$$

induit par passage au quotient une forme quadratique $q_E\colon V \to \mathbb{F}_2$, de forme bilinéaire associée a_E.

Démonstration. Soit $\pi\colon E \to E/E'$ la projection canonique. Nous définissons a_E par

$$a_E(\pi(x), \pi(y)) := \zeta([x,y])$$

Puisque $E' \subset \mathrm{Z}(E)$, a_E est bien définie. C'est une forme bilinéaire alternée (puisque $[x,x] = 1$). L'application $E \to \mathbb{F}_p$, $x \mapsto \zeta(x^p)$, définit bien une application f_E de V dans $\mathbb{F}_p$. On a $\Sigma(2) = 1$ et, pour $p \neq 2$, $\Sigma(p) \equiv 0 \pmod p$. Si $p \neq 2$ $(xy)^p = x^p y^p$, donc $f_E(\pi(x) +$

$\pi(y)) = f_E(\pi(x)) + f_E(\pi(y))$, f_E est une forme linéaire. Le groupe E est d'exposant p si tout élément $x \neq 1$ de E est d'ordre p, *i.e.*, si $f_E = 0$. Si $p = 2$, on a $(xy)^2 = x^2y^2[x, y]$, puisque $[y, x]$ est d'ordre au plus 2. Donc q_E est une forme quadratique de forme bilinéaire associée a_E. □

Corollaire 3.10. *Soit E un p-groupe extra-spécial ou un CC-groupe. Alors la forme a_E est non dégénérée, et :*

(a) *si E est un p-groupe extra-spécial, il existe un entier n tel que $|E| = p^{2n+1}$.*

(b) *si E est un CC-groupe et $p \neq 2$, il est d'exposant p.*

Démonstration.

(a) Nous supposons que E est un p-groupe extra-spécial : Si $\pi(x)$ appartient au noyau de a_E, par définition, pour tout y dans E, on a $[x, y] = 1$, donc $x \in \mathrm{Z}(E)$, et par conséquent $\pi(x) = \pi(1)$, et a_E est non dégénérée. La théorie des formes alternées montre que V est de dimension paire sur $\mathbb{F}_p$, soit $2n$ cette dimension. On a donc $|V| = p^{2n}$ et $|E| = p^{2n+1}$.

(b) Supposons maintenant que E est un CC-groupe et que $p \neq 2$. Les éléments d'ordre au plus p de E forment un sous-groupe caractéristique d'indice au plus p, et par conséquent, E est d'exposant p. L'image réciproque dans E du radical de la forme a_E est un sous-groupe caractéristique abélien p-élémentaire, et donc la forme est non dégénérée. □

CC-groupes et groupes de Heisenberg

Définition 3.11. *Soit F un corps de caractéristique différente de 2. Soit V un espace vectoriel de dimension $2n$ sur F. Soit $\langle\, ,\, \rangle$ une forme alternée non dégénérée sur V. On associe à V un groupe, noté $H(V)$, appelé* groupe de Heisenberg *de $(V, \langle\, ,\, \rangle)$ et défini de la façon suivante : $H(V)$ est l'ensemble $V \times F$, (muni de la topologie produit lorsque F est un corps topologique), et de la loi de groupe*

$$(v, t)(v', t') = (v + v', t + t' + \tfrac{1}{2}\langle v, v'\rangle).$$

Nous verrons à la proposition 3.15 que, lorsque F est un corps premier $\mathbb{F}_p$ à p éléments (p impair), le groupe $H(V)$ est un p-groupe extra-spécial.

Définition 3.12. *Soit F le corps à 2 éléments. Soit X un espace vectoriel sur F de dimension finie, X^* le dual de X. Soit Γ l'un des groupes $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ ou Q_8 (le groupe des quaternions), muni d'un monomorphisme du groupe additif de F dans Γ ; si $t \in F$, on note $\overline{t}$ son image dans Γ. Soit $E(X,\Gamma)$ le groupe défini sur $X \times X^* \times \Gamma$ par*

$$(x, \phi, \gamma)(x', \phi', \gamma') = (x + x', \phi + \phi', \gamma\gamma'\overline{\phi(x')}).$$

Remarques

(a) Si $p \neq 2$, en prenant $\Gamma = \mathbb{Z}/p\mathbb{Z}$, on peut définir un groupe $E(X;\Gamma)$ de façon analogue au cas (I-4-b) ; soit alors $V = X + Y$ un espace vectoriel symplectique sur F, X et Y des sous-espaces totalement isotropes maximaux de V, Y est isomorphe au dual de X, et les groupes $H(V)$ et $E(X,\Gamma)$ sont isomorphes.

(b) Si Γ est égal au corps à p éléments, alors le groupe $E(X,\Gamma)$ correspond à la construction donnée par André Weil [Ser99] (voir [Wei64]).

Proposition 3.13. *Un groupe E est un CC-groupe s'il est isomorphe à l'un des groupes $E(X,\Gamma)$ ci-dessus.*

Groupes de Heisenberg sur un corps fini

Définition 3.14. *Un p-groupe P est* spécial *si P est abélien élémentaire, ou si P est de classe 2 et $P' = \mathrm{Z}(P) = \Phi(P)$ est abélien élémentaire.*

Les p-groupes extra-spéciaux sont donc les p-groupes spéciaux de classe 2 et de centre de cardinal p.

La proposition suivante sera utilisée lors de l'étude du groupe des automorphismes d'un p-groupe extra-spécial.

Proposition 3.15. *Soit $(V, \langle\, ,\, \rangle)$ un espace vectoriel symplectique sur le corps fini $\mathbb{F}_q$ à q éléments ($q = p^m$, avec p impair), et $H = H(V)$ le groupe de Heisenberg qui lui est associé. Le groupe H est un p-groupe spécial d'exposant p et $[H,H] = (\mathbb{F}_q, +)$. En particulier, si $p = q$, H est extra-spécial.*

Démonstration

• Centre de H : Soit $h_0 \in \mathrm{Z}(H)$, $h_0 = (v_0, t_0)$, pour tout $h \in H$, $h = (v, t)$, on a $h_0 h = h h_0$, donc $\langle v_0, v\rangle = \langle v, v_0\rangle = -\langle v_0, v\rangle = 0$. La forme $\langle\, ,\, \rangle$ étant non dégénérée, $v_0 = 0$. Ainsi $\mathrm{Z}(H) = (\mathbb{F}_q, +)$.

• Groupe dérivé : Soient $h = (v, t)$, $h' = (v', t')$ deux éléments de H, puisque $[h, h'] = \langle v, v'\rangle$, on a $[H, H] = \mathbb{F}_q$.

• Groupe de Frattini : Pour tout $k \in \mathbb{Z}$, on a : $(v, t)^k = (kv, kt)$, donc $(v, t)^p = (0, 0)$, et H est d'exposant p. On en déduit $\Phi(H) = [H, H]$. □

Remarque. On définit aussi des groupes de Heisenberg sur un corps fini, de caractéristique éventuellement égale à 2, à partir d'un espace V, muni d'une forme $\langle\, ,\, \rangle$ dégénérée [Gér77].

Classification des p-groupes extra-spéciaux

Théorème 3.16. *Soit E un p-groupe extra-spécial d'ordre p^{2n+1}. Alors E est de l'un des types suivants.*

(a) *Si $p \neq 2$:*

(i) *Si E est d'exposant p, il a comme présentation x_i, y_i, $(1 \leqslant i \leqslant n)$*

$$x_i^p = y_i^p = [x_i, x_j] = [y_i, y_j] = [x_i, y_j] = 1 \quad (1 \leqslant i \neq j \leqslant n)$$

$$[x_i, y_i] = z, [z, x_i] = [z, y_i] = 1 \quad (1 \leqslant i \leqslant n).$$

On dit alors que E est de type p_+^{2n+1}.

(ii) *Si E est d'exposant p^2, il a comme présentation x_i, y_i, $(1 \leqslant i \leqslant n)$*

$$x_i^p = y_i^p = 1 \quad (1 \leqslant i \leqslant n-1)$$

$$[x_i, x_j] = [y_i, y_j] = [x_i, y_j] = 1 \quad (1 \leqslant i \neq j \leqslant n)$$

$$[x_i, y_i] = z,\ [z, x_i] = [z, y_i] = 1 \quad (1 \leqslant i \leqslant n),\quad x_n^p = 1,\quad y_n^p = z.$$

On dit alors que E est de type p_-^{2n+1}.

(b) *Si $p = 2$:*

(i) *Si q_E est d'indice de Witt n, E a comme présentation x_i, y_i, $(1 \leqslant i \leqslant n)$*

$$x_i^2 = y_i^2 = [x_i, x_j] = [y_i, y_j] = [x_i, y_j] = 1 \quad (1 \leqslant i \neq j \leqslant n),$$

$$[x_i, y_i] = z,\ [z, x_i] = [z, y_i] = 1 \quad (1 \leqslant i \leqslant n)$$

On dit alors que E est de type 2_+^{2n+1}.

(ii) *Si q_E d'indice de Witt $n-1$, E a comme présentation x_i, y_i,* $(1 \leqslant i \leqslant n)$

$$x_i^2 = y_i^2 = 1 \ \ (1 \leqslant i \leqslant n-1)$$
$$[x_i, x_j] = [y_i, y_j] = [x_i, y_j] = 1 \ \ (1 \leqslant i \neq j \leqslant n)$$
$$[x_i, y_i] = z, [z, x_i] = [z, y_i] = 1 \ \ (1 \leqslant i \leqslant n), \ \ x_n^2 = z, \ \ y_n^2 = z.$$

On dit alors que E est de type 2_-^{2n+1}.

Démonstration

(a) Supposons d'abord $p \neq 2$. Distinguons deux cas suivant que la forme f_E est nulle ou non.

- Si $f_E = 0$, le groupe E est d'exposant p. Soient

$$e_1, \ldots, e_n, \varepsilon_1, \ldots, \varepsilon_n$$

des vecteurs de V, formant une base symplectique, *i.e.,* tels que

$$a_E(e_i, e_j) = a_E(\varepsilon_i, \varepsilon_j) = 0,$$
$$a_E(e_i, \varepsilon_j) = \delta_{i,j}.$$

Soient x_i, y_i, $(1 \leqslant i \leqslant n)$, des éléments de E vérifiant $\pi(x_i) = e_i$ et $\pi(y_i) = \varepsilon_i$. On a

$$E = \langle x_i, y_i \mid 1 \leqslant i \leqslant n \rangle,$$

et les relations du théorème 3.16 (a) (i) sont satisfaites. On vérifie qu'un groupe engendré par x_i, y_i, pour $1 \leqslant i \leqslant n$, satisfaisant à ces relations est d'ordre p^{2n+1} et extra-spécial.

- Si $f_E \neq 0$ notons H le noyau de f_E, c'est donc un hyperplan de V. On a $H^\perp \subset H$ et $\dim H^\perp = 1$. On écrit :

$$H = W \oplus H^\perp,$$

W est un sous-espace non dégénéré de dimension $2n-2$. On a $V = W \oplus W^\perp$, avec $W^\perp = H^\perp \oplus D$; $W^\perp$ est un plan hyperbolique. Soient $e_1, \ldots, e_n, \varepsilon_1, \ldots, \varepsilon_n$, des vecteurs de V, formant une base symplectique, tels que la sous-famille $e_1, \ldots, e_{n-1}, \varepsilon_1, \ldots, \varepsilon_{n-1}$ soit une base de W, e_n engendre $H^\perp$ et ε_n engendre D. On a :

$$a_E(e_i, e_j) = a_E(\varepsilon_i, \varepsilon_j) = a_E(e_i, \varepsilon_j) = 0,$$

si $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, avec $i \neq j$, et $a_E(e_i, \varepsilon_i) = 1$ si $1 \leqslant i \leqslant n$. Soient x_i, y_i, $(1 \leqslant i \leqslant n-1)$, des éléments de E vérifiant $\pi(x_i) = e_i$, $\pi(y_i) = \varepsilon_i$. On a les relations

$$x_i^p = y_i^p = [x_i, x_j] = [y_i, y_j] = [x_i, y_j] = 1 \;\; (1 \leqslant i \neq j \leqslant n-1)$$
$$[x_i, y_i] = z, \; [z, x_i] = [z, y_i] = 1 \;\; (1 \leqslant i \leqslant n-1).$$

Enfin, soient x'_n, y'_n des éléments de E tels que $\pi(x'_n) = e_n$, $\pi(y'_n) = \varepsilon_n$. On a

$$(x'_n)^p = 1, \; (y'_n)^p \in E' \smallsetminus \{1\}, \; [x'_n, y'_n] = z.$$

On écrit : $(y'_n)^p = z^\alpha$, où $\alpha \in \mathbb{F}_p$. Posons :

$$x_n = (x'_n)^\alpha, \; y_n = (y'_n)^{\alpha^{-1}},$$

on obtient alors

$$\pi(x_n) = \alpha e_n, \; \pi(y_n) = \alpha^{-1}\varepsilon_n.$$

Puisque $W^\perp = \langle \pi(x_n), \pi(y_n) \rangle$, on a :

$$E = \langle x_i, y_i \mid 1 \leqslant i \leqslant n \rangle,$$

et les relations du théorème 3.16 (a) (ii). On vérifie qu'un groupe engendré par x_i, y_i, $1 \leqslant i \leqslant n$ satisfaisant à ces relations est d'ordre p^{2n+1} et extra-spécial. Donc, si E est extra-spécial d'ordre p^{2n+1} avec $p > 2$, alors E est de l'un des deux types précédents.

(b) On suppose maintenant que $p = 2$. Il y a deux types de formes quadratiques sur $\mathbb{F}_2$: celles d'indice de Witt n pour lesquelles les sous-espaces totalement isotropes maximaux sont de dimension n, et celles d'indice $n-1$, pour lesquelles les sous-espaces totalement isotropes maximaux sont de dimension $n-1$.

- Supposons q_E d'indice de Witt n. Soient X et Y des sous-espaces totalement isotropes maximaux de V tels que $V = X \oplus Y$. Soient $e_1, \ldots, e_n$, $\varepsilon_1, \ldots, \varepsilon_n$, des vecteurs de V, formant une base symplectique, tels que $e_1, \ldots, e_n$ soit une base de X et $\varepsilon_1, \ldots, \varepsilon_n$ une base de Y. Soient x_i, y_i, $(1 \leqslant i \leqslant n)$, des éléments de E vérifiant $\pi(x_i) = e_i$, $\pi(y_i) = \varepsilon_i$. Alors

$$E = \langle x_i, y_i \mid 1 \leqslant i \leqslant n \rangle,$$

et les relations du théorème 3.16 (b) (i) sont satisfaites. On vérifie qu'un groupe engendré par x_i, y_i, $1 \leqslant i \leqslant n$ satisfaisant à ces relations est d'ordre 2^{2n+1} et extra-spécial.

- Supposons q_E d'indice de Witt $n-1$. Soient X et Y des sous-espaces totalement isotropes maximaux de V tels que $X \cap Y = 0$. Alors $X \oplus Y$ est un sous-espace non dégénéré de V, et

$$V = (X \oplus Y) \perp V^0,$$

avec V^0 plan hyperbolique pour a_E tel que $q_E(v) \neq 0$, pour tout $v \in V^0$, $v \neq 0$. Soient x_i, y_i, des éléments de E vérifiant $\pi(x_i) = e_i$, $\pi(y_i) = \varepsilon_i$, pour $1 \leqslant i \leqslant n-1$, tels que $\pi(x_n)$, $\pi(y_n)$ soit une base de V^0, et $a_E(\pi(x_i), \pi(y_j)) = \delta_{i,j}$, pour $1 \leqslant i, j \leqslant n$. Alors

$$E = \langle x_i, y_i \mid 1 \leqslant i \leqslant n \rangle,$$

et les relations du théorème 3.16 (b) (ii) sont satisfaites. On vérifie qu'un groupe engendré par x_i, y_i, $1 \leqslant i \leqslant n$ satisfaisant à ces relations est d'ordre 2^{2n+1} et extra-spécial.

□

Le résultat suivant se déduit du théorème précédent et de la structure de l'espace V dans chaque cas.

Corollaire 3.17. *Soit E un groupe non abélien d'ordre p^3. Alors,*

(a) *si $p = 2$, E est isomorphe au groupe Q_8 des quaternions ou au groupe diédral D_4 ;*

(b) *si $p \neq 2$, E est de l'un des deux types suivants :*

- *E est d'exposant p, noté $M(p)$, avec la présentation :*

$$M(p) = \langle x, y \mid x^p = y^p = [x, [x, y]] = [y, [x, y]] = 1 \rangle$$

- *E est d'exposant p^2, noté $M_3(p)$, avec la présentation :*

$$M_3(p) = \langle x, y \mid x^{p^2} = y^p = 1,\ yxy^{-1} = x^{1+p} \rangle.$$

Produits centraux de groupes d'ordre p^3

Définition 3.18. *Un groupe G est* produit central *des sous-groupes H_i, pour $1 \leqslant i \leqslant n$, si $G = H_1 \cdot H_2 \cdots H_n$, et si, pour tout couple d'entiers (i, j) tels que $1 \leqslant i \neq j \leqslant n$, on a $[H_i, H_j] = \{1\}$.*

Remarques

(a) H_i est distingué dans G ;

(b) si $i \neq j$, on a $(H_i \cap H_j) \subset \mathrm{Z}(G)$;

(c) tout produit central $H_1 \cdots H_n$ est une image du produit $H_1 \times \cdots \times H_n$ par l'application naturelle :

$$(h_1, \ldots, h_n) \longmapsto h_1 \cdots h_n.$$

Proposition 3.19

Soient $E_1, \ldots, E_n$ des p-groupes extra-spéciaux d'ordre p^3. Alors il n'y a, à isomorphisme près, qu'un unique produit central de $E_1, \ldots, E_n$ qui a un centre d'ordre p. C'est un p-groupe extra-spécial, de cardinal p^{2n+1}, noté $E_1 \cdots E_n$, appelé le *produit central de $E_1, \ldots, E_n$.*

Ce groupe est le quotient de $E_1 \times \cdots \times E_n$ par l'hyperplan de $\mathbb{F}_p^n$ défini par exemple par $\sum_{i=1}^n x_i = 0$.

Corollaire 3.20. *Tout p-groupe extra-spécial est produit central de p-groupes non commutatifs d'ordre p^3.*

Automorphismes des p-groupes extra-spéciaux

Premières propriétés. Pour tout groupe G, on note $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs de G. On a $\mathrm{Int}(G) \simeq G/\mathrm{Z}(G)$.

Proposition 3.21. *Soit E un p-groupe extra-spécial. Alors* $\mathrm{Int}(E)$ *est constitué par les automorphismes de E qui opèrent trivialement sur E/E'.*

Démonstration. Soit X l'ensemble des les automorphismes de E qui opèrent trivialement sur E/E'. Il est immédiat que $\mathrm{Int}(E) \subset X$. Puisque $|\mathrm{Int}(E)| = p^{2n}$, p^{2n} divise $|X|$. D'autre part, soient

$$(x_i, y_i,\ 1 \leqslant i \leqslant n)$$

des éléments qui relèvent une base de V. Tout élément σ de X vérifie $\sigma(x_i) = x_i z^{\alpha_i}$ et $\sigma(y_i) = y_i z^{\beta_i}$, où $\alpha_i, \beta_i \in \mathbb{F}_p$, puisque $E' = \mathrm{Z}(E)$. La donnée des α_i, β_i déterminant σ, on obtient $|X| \leqslant p^{2n}$. Il s'ensuit que $|X| = p^{2n}$, et $\mathrm{Int}(E) = X$. □

Proposition 3.22. *Soit W un espace vectoriel de dimension finie $2n$ sur le corps $\mathbb{F}_q$, $(q = p^m)$, muni d'une forme bilinéaire $\langle\, ,\, \rangle$ alternée non dégénérée. Soient $f\colon W \to \mathbb{F}_q$ une forme linéaire non nulle et*

$$G := \left\{ g \in \mathrm{Sp}(W) \;\middle|\; f \circ g = f \right\}.$$

Alors $G = HS$, avec H distingué dans G et $H \cap S = \{1\}$, où

(a) *si $p = 2$, H est un 2-groupe abélien élémentaire d'ordre q^{2n-1} ;*
(b) *si $p \neq 2$,*
- *si $n > 1$, H est un groupe de Heisenberg ;*
- *Si $n = 1$, H est un p-groupe abélien élémentaire d'ordre q ;*

Si $n = 1$, on a $S = \{1\}$ et si $n \neq 1$ on a $S \simeq \mathrm{Sp}(2n-2, q)$.

Démonstration

(a) Notons V_0 le noyau de f, c'est un hyperplan de W. La forme bilinéaire alternée $\langle\, ,\, \rangle$ étant non dégénérée, l'orthogonal $V_0^{\perp}$ de V_0 est une droite, que l'on note D, et l'on a $D \subset V_0$. Choisissons un générateur a de D de telle sorte que $f(w) = \langle a, w\rangle$, pour tout $w \in W$. C'est possible, car l'ensemble $\mathcal{L}$ des formes linéaires $\phi : W \to \mathbb{F}_q$, dont le noyau contient V_0, est un espace vectoriel de dimension 1 sur $\mathbb{F}_q$, et l'on a

$$\mathcal{L} = \left\{ w \longmapsto \langle \lambda a, w\rangle \;\middle|\; \lambda \in \mathbb{F}_q \right\}.$$

Soit $b \in W$, tel que $f(b) = 1$. Le plan engendré par les vecteurs a et b est donc un plan hyperbolique. Soit V_1 un supplémentaire orthogonal de ce plan dans W

$$W = V_1 \oplus V_1^{\perp},\ V_1^{\perp} = \langle a, b\rangle.$$

Soit $g \in G$, on a $g(V_0) = V_0$ et $g(V_0^{\perp}) = V_0^{\perp}$. Il est clair que G est l'ensemble des éléments de $\mathrm{Sp}(W)$ qui opèrent trivialement sur W/V_0. On a $g(a) = \lambda a$, avec $\lambda \in \mathbb{F}_q$. D'autre part, $g(b) = b + v_0$, avec $v_0 \in V_0$, car G opère trivialement sur W/V_0. On en déduit

$$1 = \langle a, b\rangle = \langle g(a), g(b)\rangle = \langle \lambda a, b + v_0\rangle = \lambda.$$

Ainsi, si $g \in G$, il existe $v \in V_1$ et $t \in \mathbb{F}_q$, tels que $g(b) = ta + v + b$, et l'on a $g(a) = a$.

(b) Soit H l'ensemble des éléments de $\mathrm{Sp}(W)$ qui opèrent trivialement sur V_0/D et sur W/V_0. On a $H \subset G$ d'après la caractérisation de G. Soit $h \in H$, puisque $h \in G$, il existe $(v,t) \in V_1 \times \mathbb{F}_p$ tel que $h(b) = ta + v + b$, et l'on a $h(a) = a$. De plus, puisque h opère trivialement sur V_0/D, on a, pour tout $v_0 \in V_0$, $(h(v_0) - v_0) \in D$. On va montrer que le couple (v,t) détermine h de manière unique. Il reste à calculer les valeurs de h sur V_1 : soit $v_1 \in V_1$, $h(v_1) \in V_0$, il existe donc $t_1 \in \mathbb{F}_q$ tel que $h(v_1) = t_1 a + v_1$, car h opère trivialement sur W/V_0, et l'on a $(hv_1 - v_1) \in D$. On obtient

$$\langle h(b), h(v_1)\rangle = \langle ta + v + b, t_1 a + v_1\rangle = -t_1 + \langle v, v_1\rangle.$$

Donc, $t_1 = \langle v, v_1\rangle$, et $h(v_1) = \langle v, v_1\rangle a + v_1$. Comme a, b et V_1 engendrent W, l'élément h est uniquement déterminé par le couple (v,t) de $V_1 \times \mathbb{F}_q$. On pose donc $h = h_{(v,t)}$. Soit Φ l'application suivante :

$$\begin{aligned} \Phi : H &\longrightarrow H(V_1, 2\langle\ ,\ \rangle_1) \\ h_{(v,t)} &\longmapsto (v,t). \end{aligned}$$

On vérifie facilement que Φ est un isomorphisme de H sur le groupe de Heisenberg de l'espace symplectique $(V_1, 2\langle\ ,\ \rangle_1)$, où $\langle\ ,\ \rangle_1$ est la restriction à V_1 de la forme $\langle\ ,\ \rangle$. On peut noter que si $n = 1$ on a $V_1 = 0$ et $H = \mathbb{F}_q$.

- Détermination de S. Soit $g_1 \in \mathrm{Sp}(V_1, \langle\ ,\ \rangle_1)$. Alors, l'application linéaire $g : W \to W$, qui vérifie $g_{|V_1} = g_1$ et $g_{|V_1^\perp} = \mathrm{Id}_{V_1^\perp}$ est dans $\mathrm{Sp}(W, \langle\ ,\ \rangle)$. De plus, soit $w \in W$, $w = v_1 + v_1'$, avec $v_1 \in V_1$, $v_1' \in V_1^\perp$, alors

$$g(w) = g(v_1) + v_1'$$

et donc

$$g(w) - w = g_1(v_1) - v_1 \ \in V_1.$$

D'après la caractérisation de G, on a $g \in G$.
- Soit

$$S = \left\{ g \in \mathrm{Sp}(W, \langle\ ,\ \rangle) \;\middle|\; g_{|V_1} \in \mathrm{Sp}(V_1, \langle\ ,\ \rangle_1),\ g_{|V_1^\perp} = \mathrm{Id}_{V_1^\perp} \right\}.$$

L'ensemble S est donc un sous-groupe de G et $S = \mathrm{Sp}(V_1, \langle\ ,\ \rangle_1)$. Donc si $n > 1$ on obtient $S \simeq \mathrm{Sp}(2n-2, q)$ et si $n = 1$ on a $S = \{1\}$. De plus $H \cap S = \{1\}$. D'autre part, soit $g \in G$, pour tout $v_1 \in V_1$, on a $g(v_1) = t_1 a + w_1$, avec $t_1 \in \mathbb{F}_q$, et $w_1 \in V_1$. On vérifie facilement que l'application de V_1 dans V_1 qui à v_1 associe w_1 appartient à $\mathrm{Sp}(V_1, \langle\ ,\ \rangle_1)$. On a ainsi un morphisme surjectif de noyau H, donc $G = HS$ et H est distingué dans G. $\square$

Proposition 3.23. *Soit E un p-groupe extra-spécial. Notons B le stabilisateur de z dans $\mathrm{Aut}(E)$.*

On a la suite exacte :

$$1 \longrightarrow B \longrightarrow \mathrm{Aut}(E) \xrightarrow{\theta} \mathbb{F}_p^\times \longrightarrow 1.$$

En particulier, si $p = 2$, on a $B = \mathrm{Aut}(E)$.

Démonstration. Seule la surjectivité de θ nécessite une démonstration. Rappelons que $[x^k, y] = [x, y]^k$ dans un groupe de classe 2. Soit $k \in \mathbb{F}_p^\times$, on définit $\sigma \in \mathrm{Aut}(E)$ par $\sigma(x_i) = x_i^k$ et $\sigma(y_i) = y_i$. Alors $\sigma(z) = z^k$, puisque $z = [x_i, y_i]$. $\square$

Théorème 3.24. *Soit E un p-groupe extra-spécial d'ordre p^{2n+1}.*

(a) *Si $p = 2$, soit $\varepsilon \in \{+, -\}$, on a $\mathrm{Aut}(E)/\mathrm{Int}(E) \simeq \mathrm{O}_\varepsilon(2n, 2)$, si E est de type 2_ε^{2n+1}, où $\mathrm{O}_+(2n, 2)$, (resp. $\mathrm{O}_-(2n, 2)$, désigne le groupe orthogonal de dimension $2n$ sur $\mathbb{F}_2$ d'une forme quadratique d'indice n, (resp. $n - 1$).*

(b) *Si $p \neq 2$, on a*

- *si E est d'exposant p :*

$$B/\mathrm{Int}(E) \simeq \mathrm{Sp}(2n, p),$$

- *si E est d'exposant p^2 :*

$$B/\mathrm{Int}(E) \simeq HS,$$

où H est distingué dans $B/\mathrm{Int}(E)$ avec $H \cap S = \{1\}$, et si $n = 1$, $S = \{1\}$ et H est cyclique d'ordre p, si $n > 1$, $S \simeq \mathrm{Sp}(2n-2, p)$ et H est extra-spécial de type p_+^{2n-1}.

Démonstration. (a) Soit $\sigma \in B$, alors σ induit un automorphisme $\overline{\sigma}$ de l'espace vectoriel $V = E/E'$, associé à E, tel que $\overline{\sigma}\pi = \pi\sigma$, où π est la projection canonique de E sur V. Puisque, $\sigma \in B$, on a

$$[x, y] = \sigma([x, y]) = [\sigma(x), \sigma(y)].$$

On en déduit

$$\begin{aligned} a_E(\overline{\sigma}(\pi x), \overline{\sigma}(\pi y)) &= a_E(\pi(\sigma x), \pi(\sigma y)) \\ &= \zeta([\sigma(x), \sigma(y)]) = \zeta([x,y]) = a_E(\pi x, \pi y), \end{aligned}$$

donc :

$$\overline{\sigma} \in \mathrm{Sp}(V, a_E).$$

On a d'autre part :

$$x^p = \sigma(x^p) = (\sigma(x))^p.$$

On en déduit, si $p \neq 2$:

$$f_E(\overline{\sigma}\pi x) = f_E(\pi\sigma x) = \zeta(\sigma x)^p = \zeta(x^p) = f_E(\pi x),$$

donc

$$f_E \circ \overline{\sigma} = f_E.$$

Si $p = 2$, on a de même $q_E \circ \overline{\sigma} = q_E$. Il existe donc un morphisme λ tel que

- si $p > 2$, $\lambda\colon B \to \mathrm{Sp}(V, a_E)$;
- si $p = 2$, $\lambda\colon B \to \mathrm{O}(V, q_E)$,

défini par $\lambda(\sigma) = \overline{\sigma}$, pour tout $\sigma \in B$. D'après la proposition 3.21 que le noyau de λ est $\mathrm{Int}(E)$. Montrons la surjectivité de λ. Supposons $p = 2$. Soit $g \in \mathrm{O}(V, q_E)$, et soit (x_i, y_i), $(1 \leqslant i \leqslant n)$, un système générateur de E. Soient x_i', y_i' des éléments de E tels que $\pi(x_i') = g(\pi x_i)$, $\pi(y_i') = g(\pi y_i)$, pour $1 \leqslant i \leqslant n$. On vérifie que les x_i', y_i' satisfont aux les mêmes relations que les x_i, y_i. Soit σ l'application définie par $\sigma(x_i) = x_i'$, $\sigma(y_i) = y_i'$, pour $1 \leqslant i \leqslant n$. Cette application se prolonge en un automorphisme de E, noté encore σ, et l'on a $\lambda(\sigma) = g$. Donc λ est surjective. Si $p \neq 2$ et E d'exposant p, la démonstration est la même que dans le cas précédent. Si $p \neq 2$ et E d'exposant p^2, on va montrer que $\lambda(B) = G$, où

$$G = \left\{ g \in \mathrm{Sp}(V, a_E) \;\middle|\; f_E \circ g = f_E \right\}.$$

Soit $\sigma \in B$, on a $f_E \circ \lambda(\sigma) = f_E$, donc $\lambda(\sigma) \in G$. Soit $g \in G$. On pose $V_0 = \ker f_E$. On a $g(V_0) = V_0$, puisque $f_E \circ g = f_E$ et $g(V_0^\perp) = V_0^\perp$. Soit (x_i, y_i), $(1 \leqslant i \leqslant n)$, un système générateur de E qui vérifie les relations du théorème 3.16. Comme $V_0^\perp = \langle \pi(x_n) \rangle$, on déduit de la démonstration de la proposition 3.22 que $g(\pi(x_n)) = \pi(x_n)$. Soient x'_i, y'_i des éléments de E tels que $\pi(x'_i) = g(\pi x_i)$, $\pi(y'_i) = g(\pi y_i)$, pour $1 \leqslant i \leqslant n$. On obtient

$$E = \langle x'_i, y_i \mid 1 \leqslant i \leqslant n \rangle,$$

et les relations du théorème 3.16 (a) (ii) sont satisfaites. Il existe donc un élément σ de $\operatorname{Aut} E$, tel que, pour tout $i \in \{1, \ldots, n\}$, $\sigma(x_i) = x'_i$, $\sigma(y_i) = y'_i$. On vérifie que $\sigma \in B$ et $\lambda(\sigma) = g$. Ainsi, $\lambda(B) = G$. Et, puisque $\ker \lambda \simeq \operatorname{Int}(E)$, on a

$$B / \operatorname{Int}(E) \simeq G.$$

On applique alors les propositions 3.22 et 3.23 pour avoir la structure de $B/\operatorname{Int}(E)$.

□

Les représentations des p-groupes extra-spéciaux

Pour déterminer les représentations des p-groupes extra-spéciaux, nous allons utiliser les résultats suivants, qui sont démontrés par exemple dans [Gor68].

Définition 3.25. *Un corps K est un* corps neutralisant *pour G, si l'algèbre de groupe de G sur K, notée KG, est isomorphe à une somme directe d'algèbres de matrices sur K.*

Théorème 3.26. *Soit G un groupe fini, K un corps dont la caractéristique ne divise pas l'ordre de G, et r le nombre de classes de conjugaison de G.*

Il y a au plus r classes de KG-modules simples. Si K est un corps neutralisant pour G, en particulier si K est algébriquement clos, il y a exactement r classes de KG-modules simples.

Soient alors $d_1, \ldots, d_r$ les degrés des représentations simples non isomorphes de G. L'algèbre KG est isomorphe à la somme directe des r algèbres simples $\operatorname{End}_K(K^{d_i})$, et l'on a :

$$|G| = d_1^2 + d_2^2 + \cdots + d_r^2.$$

Théorème 3.27. *Soit $G = G_1 \times \cdots \times G_n$ un groupe fini et K un corps neutralisant pour chacun des G_i.*

Si V_i est un KG_i-module simple, $(1 \leqslant i \leqslant n)$, alors $V_1 \otimes \cdots \otimes V_n$ est un KG-module simple. Réciproquement, tout KG-module simple est de cette forme.

Théorème 3.28. *Soit $G = H_1 \cdots H_n$ un produit central de groupes finis $H_1, \dots, H_n$. Soient $G^* := H_1 \times \cdots \times H_n$, et N le noyau du morphisme $\alpha\colon G^* \to G$.*

Il y a alors une correspondance bijective entre l'ensemble des représentations de G sur un corps K et l'ensemble des représentations de G^* sur K, qui ont N dans leur noyau.

Théorème 3.29. *Soit E un p-groupe extra-spécial d'ordre p^{2n+1}. Soit K un corps de caractéristique nulle ou première à p, qui contient une racine primitive p^2-ème de 1.*

Alors

(a) *K est un corps neutralisant pour E ;*

(b) *E a exactement $p^{2n} + p - 1$ représentations irréductibles non équivalentes sur K, p^{2n} sont de degré 1 et $p - 1$ de degré p^n.*

Démonstration. La première étape consiste à déterminer les classes de conjugaison de E. Puisque le centre de E est d'ordre p, il y a p classes de conjugaison de cardinal 1. Si $x \in E \smallsetminus \mathrm{Z}(E)$, la classe de x, notée $\mathrm{cl}(x)$, est $\{xz^\alpha \mid \alpha \in \mathbb{F}_p\}$. Donc $|\,\mathrm{cl}(x)| = p$, et $E \smallsetminus \mathrm{Z}(E)$ contient $(p^{2n+1} - p)/p = p^{2n} - 1$ classes de conjugaison. Ainsi, E contient $p^{2n} + p - 1$ classes de conjugaison.

Soit $\overline{K}$ une clôture algébrique de K. D'après 3.26, E a $p^{2n} + p - 1$ représentations irréductibles non équivalentes sur $\overline{K}$, et p^{2n} de celles-ci sont de degré 1 puisque $|E/E'| = p^{2n}$. Il est clair que les représentations de degré 1 de E s'écrivent dans K. On va maintenant construire $p-1$ représentations inéquivalentes de degré différent de 1 de E. Soit ω une racine primitive p^2-ème de 1.

– Nous allons d'abord considérer le cas des groupe d'ordre p^3.

• Supposons $p = 2$. Le groupe E est de type D_4 ou Q_8. Alors les matrices

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$$

engendrent un sous-groupe de $\mathrm{GL}(2, K)$, isomorphe à D_4 si $\varepsilon = 1$ et à Q_8 si $\varepsilon = -1$. Ainsi, K^2 est un KE-module simple.

Remarque. Dans le cas de D_4, on peut prendre les matrices suivantes :

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ces matrices, étant écrites sur $\mathbb{Z}$, donnent des représentations simples de D_4 pour n'importe quel corps premier différent de $\mathbb{F}_2$, et en particulier pour $\mathbb{Q}$.

- Supposons $p \neq 2$. Le groupe E est de type $M_3(p)$ ou $M(p)$. On a

$$M_3(p) = \langle x, y \mid x^{p^2} = y^p = 1,\ yxy^{-1} = x^{1+p} \rangle$$

Soient ρ_i, $(1 \leqslant i \leqslant p-1)$, des homomorphismes

$$\rho_i \colon E \longrightarrow \mathrm{GL}(p, K),$$

qui vérifient

$$\rho_i(x) = \begin{pmatrix} \omega^i & & & & \\ & \ddots & & & \\ & & \omega^{i(1+kp)} & & \\ & & & \ddots & \\ & & & & \omega^{i(1+(p-1)p)} \end{pmatrix}, \quad \rho_i(y) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

On vérifie que ρ_i établit un isomorphisme entre E et un sous-groupe du groupe $\mathrm{GL}(p, K)$ qui ne stabilise aucun sous-espace propre de K^p. Donc, chaque ρ_i est une représentation irréductible de E. Comme $\rho_i(x^p) = \omega^{ip} = \rho_i(z)$ est une matrice scalaire, les représentations ρ_i et ρ_j sont non équivalentes si $i \neq j$. Chaque ρ_i donne ainsi une représentation irréductible de E sur $\overline{K}$, de degré p. Nous avons donc obtenu $p-1$ représentations irréductibles de E sur $\overline{K}$, de degré différent de 1.

On a

$$M(p) = \langle x, y \mid x^p = y^p = [x,[x,y]] = [y,[x,y]] = 1 \rangle.$$

Posons $\eta = \omega^p$. On remarque que, dans ce cas, la présence d'une racine p-ème de l'unité suffit. Soient ρ_i, $(1 \leqslant i \leqslant p-1)$, des homomorphismes

$$\rho_i \colon E \longrightarrow \mathrm{GL}(p, K),$$

qui vérifient

$$\rho_i(x) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \eta^{ki} & & \\ & & & \ddots & \\ & & & & \eta^{(p-1)i)} \end{pmatrix}, \qquad \rho_i(y) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

Et, $\rho_i(z) = \eta^i$ Id, car $z = [x, y]$. On conclut alors comme précédemment.

– Cas général : Pour déterminer toutes les représentations des p-groupes extra-spéciaux, on utilise le fait que ces groupes sont des produits centraux de p-groupes extra-spéciaux d'ordre p^3 d'après la proposition 3.9, ainsi que les théorèmes 3.27 et 3.28. Comme la dimension sur K d'un produit tensoriel d'espaces vectoriels est le produit de leurs dimensions, la conclusion résulte immédiatement de l'étude des représentations des p-groupes extra-spéciaux d'ordre p^3. □

Modèles de représentations irréductibles de p-groupes extra-spéciaux

Théorème 3.30. *Soit E un p-groupe extra-spécial. Soit A un sous-groupe commutatif maximal de E et ψ une représentation non triviale de $\mathrm{Z}(E)$ sur $\mathbb{C}$.*

Si α est une représentation linéaire de A qui vérifie $\alpha_{|\,\mathrm{Z}(E)} = \psi$, alors la représentation induite de A à E, notée α^E, est irréductible.

Démonstration. On a $\mathrm{Z}(E) \subset A$ et $|A| = p^{n+1}$, puisqu'un sous-espace isotrope maximal de E, pour a_E, est de dimension n. Soit α une représentation linéaire de A, qui vérifie :

$$\alpha_{|\,\mathrm{Z}(E)} = \psi\ .$$

Soit α^E la représentation induite de α de A à E. Elle est de degré $[E : A] = p^n$. Si α^E était réductible, alors α^E serait somme de représentations de degré 1 de E, et l'on aurait $z \in \ker(\alpha^E)$, car toutes les représentations de degré 1 de E ont z dans leur noyau. Or, puisque $\alpha(z) \neq 1$ (car ψ n'est pas triviale), on a $\alpha^E(z) \neq 1$, et α^E est irréductible. □

Corollaire 3.31. *Les représentations irréductibles de degré > 1 d'un p-groupe extra-spécial E sont fidèles et peuvent être obtenues comme induites de représentations linéaires d'un sous-groupe commutatif maximal de E, dont la restriction à $\mathrm{Z}(E)$ est un caractère non trivial de $\mathrm{Z}(E)$.*

Démonstration

Soit A un sous-groupe maximal de E. Pour $i \in \{1, \ldots, p-1\}$, soit α_i une représentation linéaire de A, dont la restriction à $\mathrm{Z}(E)$ est égale à un caractère ψ_i non trivial de $\mathrm{Z}(E)$. (On obtient tous les caractères non triviaux de $\mathrm{Z}(E)$ de cette manière.)

Soit α_i^E la représentation induite de α_i de A à E. Elle est de degré p^n. Puisque le caractère ψ_i n'est pas trivial, on a $\mathrm{Z}(E) \cap \ker(\alpha_i^E) = \{1\}$. On en déduit $\ker(\alpha_i^E) = \{1\}$, *i.e.*, α_i^E est fidèle. D'après la proposition précédente, α_i^E est irréductible. Si $i \neq j$, les représentations α_i^E et α_i^E ne sont pas équivalentes. Nous avons ainsi obtenu $p-1$ représentations irréductibles de E de degré 1 et non équivalentes. Toutes les représentations irréductibles de degré 1 de E sont donc de cette forme. $\square$

Les représentations des groupes de Heisenberg

Les résultats précédemment obtenus pour les représentations des p-groupes extra-spéciaux admettent des analogues dans le cas des groupes de Heisenberg. Le théorème suivant est l'analogue sur les corps finis du théorème de Stone von Neumann[(5)].

Théorème-Définition 3.32. *Soient F un corps fini de caractéristique impaire et $\psi \colon F \to \mathbb{C}^\times$ un caractère non trivial de F et V un espace*

[(5)]Le théorème de Stone von Neumann dit que le groupe de Heisenberg réel possède une seule représentation unitaire continue irréductible qui est l'identité sur le centre (la réalisation classique de cette représentation est appelée la représentation de Schrödinger). On obtient donc une représentation projective de $\mathrm{Sp}(2n, \mathbb{R})$ qui fournit une représentation (dite *métaplectique*) unitaire continue du revêtement à deux feuillets de $\mathrm{Sp}(2n, \mathbb{R})$, appelé *groupe métaplectique* (voir [Sha62], [Wal77, chap. 5], [LV80], [Mac89], [vN96] et [KM90]). Une généralisation aux corps localement compacts non discrets a été réalisée par André Weil dans [Wei64] (voir aussi [MVW87]).

vectoriel de dimension finie sur F, muni d'une forme alternée non dégénérée $\langle\ ,\ \rangle$.

Alors à isomorphisme près, il existe une unique représentation irréductible (ρ, S) du groupe de Heisenberg $H := H(V)$ (associé à V) telle que :

$$\rho\big((0,t)\big) = \psi(t)\,\mathrm{Id}_S \quad \forall t \in F.$$

La représentation (ρ, S) est appelée la représentation de Weil *de $H(V)$ associée à ψ.*

Démonstration. Pour $t \in F$, nous notons $\mathrm{Tr}(t)$ la trace de t sur $\mathbb{F}_p$, *i.e.,* la trace de l'endomorphisme de $\mathbb{F}_p$-espaces vectoriels $a \mapsto ta$. Comme le groupe de Galois $\mathrm{Gal}(F/\mathbb{F}_p)$ de F sur $\mathbb{F}_p$ est engendré par l'automorphisme de Frobenius $t \mapsto t^p$, il vient

$$\mathrm{Tr}(t) = \sum_{\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)} \sigma(t) = \sum_{i=0}^{[F:\mathbb{F}_p]-1} t^{p^i}.$$

Soit maintenant ζ une racine primitive p-ième de l'unité dans $\mathbb{C}$. On définit une représentation ψ de degré 1 (*i.e.,* un caractère) de F sur $\mathbb{C}$ par

$$\psi(t) := \zeta^{\mathrm{Tr}(t)}.$$

Comme l'application trace est non dégénérée (*i.e.,* $\mathrm{Tr}(ta) = 0$ pour tout $t \in F$ si et seulement si $a = 0$), l'application $t \mapsto (t' \mapsto \zeta^{\mathrm{Tr}(tt')})$ définit un isomorphisme de F sur $\mathrm{Hom}(F, \mathbb{C}^\times) =: \widehat{F}$. Par conséquent, le caractère ψ est de la forme $\psi(t) = \zeta^{\mathrm{Tr}(at)}$ pour un certain $a \in F \smallsetminus \{0\}$.

Nous notons $(\ |\ )$ le produit scalaire usuel sur F^n :

$$(x|y) := \sum_{i=1}^{n} x_i y_i.$$

La trace et le produit scalaire étant non dégénérés, l'application $z \mapsto \widehat{z}$, définie par

$$\widehat{z}(y) := \zeta^{\mathrm{Tr}((x|y))},$$

est un isomorphisme de F^n sur $\mathrm{Hom}(F^n, \mathbb{C}^\times) =: \widehat{F^n}$.

Nous identifions V à F^{2n}. La forme $\langle\, ,\, \rangle$ définie par

$$\langle v, v' \rangle := \sum_{i=1}^{n} v_i v'_{n+i} - v_{n+i} v'_i$$

est une forme alternée non dégénérée sur V. La loi de groupe dans H s'écrit alors :

$$(x, y, t)(x', y', t') = (x + x', y + y', t + t' + \tfrac{1}{2}((x|y') - (y|x'))).$$

Nous désignons par $\mathbb{C}^{F^n}$ l'espace des fonctions de F^n dans $\mathbb{C}$. Nous définissons une représentation $\rho = \rho_\psi$ de H (d'espace $\mathbb{C}^{F^n}$) par

$$\rho(x, y, t) f(z) \ := \ \psi\Big(t + (y|z) + \frac{1}{2}(x, y)\Big) f(z + x),$$

pour tout $f \in \mathbb{C}^{F^n}$.

Nous allons d'abord vérifier que le support du caractère de ρ est le centre de H. Soit $(\delta_u)_{u \in F^n}$ la base de $\mathbb{C}^{F^n}$ définie par $\delta_u(z) := \delta_{u,z}$, où $\delta_{u,z}$ est le symbole de Kronecker. Nous obtenons

$$\begin{aligned} \rho(x, y, t)\delta_u(z) &= \psi(t + (y|z) + \frac{1}{2}(x|y))\delta_u(z + x) \\ &= \psi(t + (y|u - x) + \frac{1}{2}(x|y)\delta_{u-x}(x). \end{aligned}$$

Il s'ensuit que le caractère χ_ρ de ρ est nul si $x \neq 0$. D'autre part,

$$\chi_\rho(0, y, t) = \sum_{z \in F^n} \psi(t + (y|z)) = \psi(t) \sum_{\widehat{z} \in \widehat{F^n}} \widehat{z}(y) = |F^n| \psi(t) \delta_{y,0}.$$

Nous avons donc $\chi_\rho(0, y, t) = 0$ si $y \neq 0$ et $|\chi_\rho(0, 0, t)| = |F^n|$.

D'autre part, puisque

$$\frac{1}{|H|} \sum_{(x,y,t) \in H} |\chi_\rho(x, y, t)|^2 = \frac{1}{|F^{2n+1}|} \sum_{t \in F} |F^n|^2 = 1,$$

la représentation ρ est irréductible.

Nous sommes maintenant en mesure de décrire la classification des représentations irréductibles de H. Parmi celles-ci, les représentations de degré 1 sont des morphismes à valeur dans le groupe commutatif $\mathbb{C}^\times$, donc sont triviales sur le groupe dérivé de H, lequel est l'ensemble des éléments de la forme $(0, 0, t)$ avec $t \in F$. Les représentations de H de degré 1 sont donc les représentations η_χ définies par

$\eta_\chi(v) := \chi(v)$, avec $\chi \in \widehat{F^{2n}}$. Rappelons que deux représentations irréductibles sont isomorphes si et seulement si elles ont même caractère (voir [Ser78, I.2.3. Cor. 2]). Les représentations ρ_ψ et $\rho_{\psi'}$ (resp. η_χ et $\eta_{\chi'}$) ne sont donc pas isomorphes si $\psi \neq \psi'$ (resp. $\chi \neq \chi'$).

On a

$$\sum_{\psi \in \widehat{F} \smallsetminus \{1\}} \deg(\rho_\psi)^2 + \sum_{\chi \in \widehat{F^{2n}}} \deg(\eta_\chi)^2 = (|F|-1)|F^n|^2 + |F^{2n}| = |H|.$$

Comme la somme des carrés des degrés de toutes les représentations irréductibles d'un groupe fini est égale au cardinal du groupe (voir [Ser78, I.2.4. Cor. 2]), nous en déduisons que les représentations irréductibles de H sont les η_χ pour χ parcourant $\widehat{F^{2n}}$ et les ρ_ψ, pour ψ parcourant $\widehat{F} \smallsetminus \{1\}$. $\square$

Soit A_0 un sous-groupe de V. Nous posons

$$A_0^\perp = \left\{ v \in V \;\middle|\; \forall a \in A_0 \quad \psi\big(\langle v, a\rangle\big) = 1 \right\}.$$

Nous supposons que $A_0 = A_0^\perp$. Soit alors

$$A := A_0 \times F \subset H.$$

L'image de A dans $H/\ker\psi$ est un sous-groupe abélien maximal de $H/\ker\psi$.

Modèle de Schrödinger. Soit $V = X \oplus Y$ une *polarisation complète* (*i.e.,* X et Y sont des sous-espaces totalement isotropes maximaux de V). Posons $A_0 = X$. Nous étendons le caractère ψ en un caractère ψ_X de $A = X + \mathrm{Z}(H)$, en faisant agir ψ_X trivialement sur X. Alors ρ peut être réalisée comme la représentation induite de ψ_X de A à H. L'espace S de cette représentation induite est formé des fonctions $f\colon H \to \mathbb{C}$ telles que :

$$f(ah) = \psi(a)f(h) \quad \forall a \in A,\, \forall h \in H,$$

et, l'action est donnée par la translation à droite $\rho(h)f(h') = f(h'h)$. Si $q = p$ on retrouve la situation du théorème 3.30.

Nous allons déduire de ρ_ψ une représentation projective α de $\mathrm{Sp}(V)$

$$\alpha\colon\ \mathrm{Sp}(V) \longrightarrow \mathrm{PGL}(S)\ .$$

En effet, le groupe symplectique $\mathrm{Sp}(V)$ agit sur H par :

$$g \cdot (v,t) = (gv,t), \quad \text{pour } g \in \mathrm{Sp}(V),\ v \in V \text{ et } t \in F.$$

Puisque l'action de $\mathrm{Sp}(V)$ sur H est triviale sur $\mathrm{Z}(H)$, elle conserve chaque caractère du centre. Pour $g \in \mathrm{Sp}(V)$, l'application $h \mapsto \rho_\psi(gh)$, notée $\rho_\psi \circ g$, est une représentation de H dans S, de caractère central ψ, vérifiant les conditions du théorème 3.32. Elle est donc équivalente à la représentation ρ_ψ, *i.e.*, il existe $M_g \in \mathrm{GL}(S)$ tel que

$$M_g\, \rho_\psi\, M_g^{-1} = \rho_\psi \circ g. \tag{3.33}$$

La représentation ρ_ψ étant irréductible, le lemme de Schur montre que M_g est bien déterminé, aux homothéties près. On en déduit une représentation projective de $\mathrm{Sp}(V)$. Notons $\widetilde{\mathrm{Sp}}_\psi$ le sous-groupe de $\mathrm{Sp}(V) \times \mathrm{GL}(S)$ formé des couples (g, M_g) vérifiant l'équation (3.33). À isomorphisme près, le groupe $\widetilde{\mathrm{Sp}}_\psi$ est indépendant de la réalisation de ρ_ψ. On a la suite exacte

$$1 \longrightarrow \mathbb{C}^\times \longrightarrow \widetilde{\mathrm{Sp}}_\psi \longrightarrow \mathrm{Sp}(V) \longrightarrow 1. \tag{3.34}$$

Le groupe $\widetilde{\mathrm{Sp}}_\psi$ est appelé le *groupe métaplectique*.

Le choix des opérateurs M_g détermine un 2-cocycle sur $\mathrm{Sp}(V)$ à valeurs dans $\mathbb{C}^\times$. En fait cette extension est scindée : puisque

$$H^2(\mathrm{Sp}(V), \mathbb{C}^\times) = \{0\},$$

il existe un homomorphisme $\mathrm{Sp}(V) \to \widetilde{\mathrm{Sp}}_\psi$ qui scinde la suite exacte (3.34). De plus, à l'exception du cas $F = \mathbb{F}_3$, $\dim_F V = 2$, cet homomorphisme est unique. En effet, sauf dans ce cas, le groupe symplectique est engendré par ces commutateurs, et n'a donc pas de caractère non trivial. On exclut provisoirement ce cas. Le composé de l'homomorphisme de $\mathrm{Sp}(V)$ dans $\widetilde{\mathrm{Sp}}_\psi$ qui scinde la suite exacte (3.34) avec la projection de $\widetilde{\mathrm{Sp}}_\psi$ sur $\mathrm{GL}(S)$ est une représentation de $\mathrm{Sp}(V)$, appelée représentation de Weil (voir [Gér77], [How73], [PSA96], [AMR96]), notée ω_ψ

$$\begin{aligned} \omega_\psi\colon \mathrm{Sp}(V) &\longrightarrow \quad \widetilde{\mathrm{Sp}}_\psi \quad \longrightarrow \mathrm{GL}(S) \\ g &\longmapsto (g, M_g) \longmapsto \quad M_g. \end{aligned}$$

Dans le cas particulier où $F = \mathbb{F}_3$, $\dim_F V = 2$, on doit choisir l'homomorphisme de $\mathrm{Sp}(V)$ dans $\widetilde{\mathrm{Sp}}_\psi$. (On le choisira tel que la représentation ω_ψ qui s'en déduit soit donnée sur les éléments unipotents supérieurs par les formules usuelles quand on la réalise dans un modèle de Schrödinger). Il existe une construction élémentaire de la représentation de Weil (voir [Neu02]).

Le cas d'un 2-groupe extra-spécial de type 2_+^{2n+1}. Nous allons voir que la situation pour un 2-groupe extra-spécial de type 2_+^{2n+1} présente des analogies avec celle d'un groupe de Heisenberg, que nous venons d'étudier. Résumons dans le théorème suivant les résultats obtenus.

Théorème 3.35. *Soit E un 2-groupe extra-spécial de type 2_+^{2n+1}. Alors $\mathbb{Q}$ est un corps neutralisant pour E et il existe, à équivalence près, une unique représentation irréductible sur $\mathbb{Q}$ et de degré différent de 1. Cette représentation est fidèle.*

En particulier, le théorème 3.35 fournit un analogue dans la situation considérée ici du théorème de Stone von Neumann.

Notons ρ la représentation définie par le théorème 3.35 et S le $\mathbb{Q}E$-module qui lui correspond. Nous allons, comme ci-dessus, déduire de ρ une représentation projective de $\mathrm{Aut}(E)$. Pour tout $g \in \mathrm{Aut}(E)$, l'application $x \mapsto \rho(gx)$, notée $\rho \circ g$, est une représentation irréductible de E. Puisque la représentation $\rho \circ g$ est équivalente à la représentation ρ, il existe $M_g \in \mathrm{GL}(S)$ tel que

$$M_g \, \rho \, M_g^{-1} = \rho \circ g.$$

Comme ρ est irréductible, le lemme de Schur montre que M_g est bien déterminé, aux homothéties près. On a donc un homomorphisme

$$\alpha\colon \mathrm{Aut}(E) \longrightarrow \mathrm{PGL}(S),$$

où $\mathrm{PGL}(S)$ désigne le quotient de $\mathrm{GL}(S)$ par son centre (le groupe $\mathrm{PGL}(S)$ est appelé le *groupe projectif linéaire*).

De plus α est injectif, puisque ρ est fidèle. Notons A l'image de l'algèbre $\mathbb{Q}E$ dans $\mathrm{End}_{\mathbb{Q}}(S)$. On identifie E à son image dans A. Il existe un sous-groupe M du normalisateur de E dans A^*, tel que :

$M/\operatorname{Z}(E) \sim \operatorname{Aut}(E)$. Par analogie avec le cas du groupe de Heisenberg, le groupe M est appelé *groupe métaplectique*. On en déduit la suite exacte

$$1 \longrightarrow E \longrightarrow M \longrightarrow \operatorname{Aut}(E)/\operatorname{Int}(E) \longrightarrow 1.$$

Puisque le quotient $\operatorname{Aut}(E)/\operatorname{Int}(E)$ est isomorphe au groupe orthogonal $\mathrm{O}_+(2n, 2)$, on a la suite exacte

$$1 \longrightarrow E \longrightarrow M \longrightarrow \mathrm{O}_+(2n, 2) \longrightarrow 1.$$

Cette suite exacte n'est pas scindée.

Application au groupe de Conway. En 1967, John Leech a construit dans [Lee67] un réseau Λ (*le réseau de Leech*) de $\mathbb{R}^{24}$ euclidien en liaison avec le problème d'empilement de sphères. Le réseau Λ est entier, pair (*i.e.,* le carré de la distance entre deux points de Λ est toujours un entier pair) et unimodulaire. En étudiant le groupe des automorphismes de Λ, John Conway découvrit l'année suivante trois nouveaux groupes finis simples (voir [Con69b] et [Con69a]). Le groupe des automorphismes de Λ, noté $.\,\mathrm{O}$ n'est pas un groupe simple, mais son centre est $\{-1, +1\}$, et le groupe quotient $.1 := .\,\mathrm{O}/\{-1, +1\}$ est un groupe simple d'ordre $2^{21}3^9 5^4 7^2 11 \cdot 13 \cdot 23$. Parmi les facteurs de composition des stabilisateurs de sous-réseaux, John Conway découvrit deux autres groupes finis simples : le groupe noté $.2$ d'ordre $2^{18}3^6 5^3 7 \cdot 11 \cdot 23$ et le groupe noté $.3$ d'ordre $2^{10}3^7 5^3 7 \cdot 11 \cdot 23$.

Posons $V := \Lambda/2\Lambda = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. C'est un $\mathbb{F}_2$-espace vectoriel de dimension 24. Il est naturellement muni d'une forme quadratique q donnée par $q(\overline{\lambda}) := \frac{1}{2}\overline{(\lambda, \lambda)}$. La forme alternée associée est non dégénérée. Soit E l'extension centrale de V par $\mathbb{Z}/2\mathbb{Z}$, associée à q. On a vu qu'un tel groupe est extra-spécial. On a la suite exacte :

$$1 \longrightarrow V \longrightarrow \operatorname{Aut}(E) \xrightarrow{\Phi} \mathrm{O}(q) \longrightarrow 1.$$

4. Les représentations complexes du groupe symétrique

La théorie des représentations complexes du groupe symétrique a été initiée par Young, Schur et Frobenius et de nombreuses notions leur sont donc attribuées. Il y a une littérature abondante sur le groupe symétrique et ses représentations complexes. Citons les livres

[Ful97], [FH91], [Jam78], [JK81], [Kir74, § 16.2], [Sag01], [Zel81]. Pour les énoncés non démontrés ci-dessous, nous nous référerons à [Ful97].

Diagrammes, sous-groupes et représentations de Young

Nous appelons *partition* d'un entier n toute suite décroissante d'entiers positifs ou nuls

$$\nu = (n_1 \geqslant n_2 \geqslant \cdots \geqslant n_k \geqslant 0) \text{ telle que } \sum_{i=1}^{k} n_i = n;$$

deux suites qui diffèrent seulement par leur nombre de zéros sont identifiées. Le nombre de n_i non nuls est appelé la *longueur* de la partition ν. Nous noterons $\mathcal{P}(n)$ l'ensemble des partitions de l'entier n.

Un *diagramme de Young* est une collection de boîtes disposées en rangées alignées à gauche avec un nombre décroissant de boîtes dans chaque rangée. Le nombre total n de boîtes est appelé la *taille* du diagramme. La liste des nombres de boîtes dans chaque rangée fournit une partition de l'entier n.

Réciproquement, à toute partition de n est associé un diagramme de Young de la manière suivante. Soit ν une partition de n. Le diagramme de Young D^ν associé à ν est défini par :

$$D^\nu := \{(i,j) \in \mathbb{N}^* \times \mathbb{N}^* \; : \; j \leqslant n_i\},$$

où $\mathbb{N}^*$ désigne l'ensemble des nombres entiers strictement positifs. Lorsque nous dessinons les diagrammes de Young, nous supposons donc que l'axe des i est dirigé vers le bas et l'axe des j est dirigé vers la droite. Soit i_0 une entier fixé. L'ensemble des points $(i_0, j) \in D^\nu$ est appelé la i_0-ème ligne de D^ν.

L'intérêt de considérer un diagramme de Young plutôt qu'une simple partition est de pouvoir mettre quelque chose dans les boîtes. Toute manière de mettre un nombre entier positif dans chacune des boîtes d'un diagramme de Young sera appelée un *remplissage* de celui-ci ; si les nombres mis dans les boîtes sont tous distincts, nous parlerons de *numérotation* du diagramme de Young. Le diagramme sera appelé la *forme* du remplissage ou de la numérotation. Une numérotation d'un diagramme de Young de taille n comprenant les nombres $1, 2, \ldots, n$, sera appelée une *numérotation standard.*

Nous appellerons *tableau de Young* tout remplissage d'un diagramme de Young tel que les nombres mis

- croissent dans chaque ligne ;
- croissent strictement dans chaque colonne.

Nous appellerons *tableau standard* tout tableau de Young dans lequel les entrées sont les nombres $1, 2, \ldots, n$, chacun apparaissant exactement une fois.

Le *groupe symétrique* $\mathfrak{S}_n$ est le groupe des permutations de l'ensemble $\{1, 2, \ldots, n\}$. Soit $\mathcal{T}_n$ l'ensemble des numérotations des diagramme de Young de taille n. Le groupe symétrique $\mathfrak{S}_n$ agit sur l'ensemble $\mathcal{T}_n$: pour une numérotation $T \in \mathcal{T}_n$ et une permutation $\sigma \in \mathfrak{S}_n$, on définit $\sigma \cdot T$ comme la numérotation consistant à mettre le nombre $\sigma(i)$ dans la boîte contenant le nombre i dans la numérotation T. Pour $T \in \mathcal{T}_n$, soit $L(T)$ le sous-groupe de $\mathfrak{S}_n$ formé des permutations qui permutent entre elles les entrées de chacune des lignes. Si $\nu = (\nu_1 \geqslant \nu_2 \geqslant \cdots \geqslant \nu_k > 0)$ est la partition de n définissant la forme de T, alors $L(T)$ est le produit direct des groupes symétriques $\mathfrak{S}_{\nu_i}$ pour $i \in \{1, 2, \ldots, k\}$, c'est-à-dire, $L(T) = \mathfrak{S}_{\nu_1} \times \mathfrak{S}_{\nu_2} \cdots \times \mathfrak{S}_{\nu_k}$. Ces sous-groupes sont appelés les *sous-groupes de Young*.

De manière analogue, nous noterons $C(T)$ le groupe des permutations permutant entre elles les entrées de chacune des colonnes. Ces sous-groupes sont compatible à l'action :

$$L(\sigma \cdot T) = \sigma \cdot L(T) \cdot \sigma^{-1} \quad \text{et} \quad C(\sigma \cdot T) = \sigma \cdot C(T) \cdot \sigma^{-1}.$$

Nous dirons que deux numérotations standard d'un diagramme de Young de taille n sont équivalentes si les lignes correspondantes possèdent les mêmes entrées. Nous appellerons *tabloïde* une classe d'équivalence de numérotations standard. Le tabloïde défini par une numérotation T sera noté $\{T\}$. Il est clair que $\{T\} = \{T'\}$ si et seulement s'il existe $\sigma \in L(T)$ telle que $T' = \sigma \cdot T$. Le groupe symétrique $\mathfrak{S}_n$ agit sur l'ensemble des tabloïdes par

$$\sigma \cdot \{T\} := \{\sigma \cdot T\}.$$

Soit $A := \mathbb{C}\mathfrak{S}_n$ l'anneau de groupe de $\mathfrak{S}_n$, formé des combinaisons linéaires complexes $\sum x_\sigma \sigma$, la multiplication étant définie par la composition dans $\mathfrak{S}_n$. Une représentation de $\mathfrak{S}_n$ est un A-module à gauche. Étant donné une numérotation standard T d'un diagramme de Young de taille n, nous définissons les deux éléments suivants de A :

$$a_T := \sum_{\sigma' \in L(T)} \sigma' \quad \text{et} \quad b_T := \sum_{\sigma'' \in C(T)} \operatorname{sgn}(\sigma'')\, \sigma''.$$

Les éléments a_T, b_T et leur produit $c_T := a_T \cdot b_T$ sont appelés les *symétriseurs de Young*.

Remarques 4.1

(a) On a $\sigma' \cdot a_T = a_T \cdot \sigma'$ et $\sigma'' \cdot b_T = b_T \cdot \sigma'' = \operatorname{sgn}(\sigma'') b_T$, pour tout $\sigma' \in L(T)$ et tout $\sigma'' \in C(T)$ (on utilise le fait que $L(T)$ et $C(T)$ sont des sous-groupes de $\mathfrak{S}_n$ et que $\operatorname{sgn}(\sigma''_1 \cdot \sigma''_2) = \operatorname{sgn}(\sigma''_1)\operatorname{sgn}(\sigma''_2)$).

(b) On a $a_T \cdot a_T = |L(T)|\, a_T$ et $b_T \cdot b_T = |C(T)|\, b_T$ (on utilise le fait que tout élément d'un sous-groupe S de $\mathfrak{S}_n$ peut s'écrire de $|S|$ manières différentes comme un produit de deux éléments de S).

Nous associons à toute partition ν de n, l'espace vectoriel complexe M^ν de base les tabloïdes $\{T\}$ de forme ν. Puisque le groupe $\mathfrak{S}_n$ agit sur l'ensemble des tabloïdes, il agit sur M^ν, lequel est donc un A-module à gauche. Nous associons à toute numérotation standard T de ν l'élément v_T de M^ν défini par

$$v_T := b_T \cdot \{T\} = \sum_{\sigma'' \in C(T)} \operatorname{sgn}(\sigma'')\, \{\sigma'' \cdot T\}.$$

Le sous-espace S^ν de M^ν engendré par les élément v_T lorsque T décrit toutes les numérotations standard de ν est appelé le *module de Specht* associé à ν. Puisque $C(\sigma \cdot T) = \sigma \cdot C(T) \cdot \sigma^{-1}$ et $\operatorname{sgn}(\sigma \cdot \sigma'' \cdot \sigma^{-1}) = \operatorname{sgn}(\sigma'')$, on a

$$v_{\sigma \cdot T} = \sum_{\sigma' \in C(T)} \operatorname{sgn}(\sigma'')\{\sigma \cdot \sigma'' \cdot T\} = \sigma \cdot v_T.$$

On a donc $\sigma \cdot v_T = v_{\sigma \cdot T}$ pour toute numérotation standard T de ν et tout $\sigma \in \mathfrak{S}_n$.

Le module de Specht S^ν est donc stable par $\mathfrak{S}_n$, autrement dit, S^ν est un sous-A-module de M^ν. Il s'ensuit que $S^\nu = A \cdot v_T$, avec T une numérotation standard de ν.

Exemples. Le module de Specht $S^{(n)}$ est la *représentation triviale* de $\mathfrak{S}_n$, c'est-à-dire, l'espace vectoriel $\mathbb{C}$ muni de l'action $\sigma \cdot z := z$, pour tout $\sigma \in \mathfrak{S}_n$ et tout $z \in \mathbb{C}$.

Le module de Specht $S^{(1^n)}$ est la *représentation alternée* (de dimension un) de $\mathfrak{S}_n$, c'est-à-dire, l'espace vectoriel $\mathbb{C}$ muni de l'action $\sigma \cdot z := \operatorname{sgn}(\sigma)\, z$, pour tout $\sigma \in \mathfrak{S}_n$ et tout $z \in \mathbb{C}$.

Aucun des modules S^ν n'est nul (car les v_T sont tous non nuls). Si ν et ν' sont deux partitions distinctes de n, alors les modules de Specht S^ν et $S^{\nu'}$ sont non isomorphes.

Les S^ν sont des modules irréductibles et nous avons ainsi associé une représentation irréductible à chaque partition de l'entier n. Puisque l'ensemble des classes de conjugaison d'un groupe fini G et celui de ses représentations irréductibles complexes ont même nombre d'éléments, et que le nombre de classes de conjugaison dans $\mathfrak{S}_n$ est égal au nombre de partitions de l'entier n, nous avons obtenu toutes les représentations irréductibles de $\mathfrak{S}_n$. En particulier, les représentations irréductibles de $\mathfrak{S}_n$ sont paramétrées par les diagrammes de Young, exactement comme le sont les classes de conjugaison.

Ordre partiel sur les partitions. Nous définissons un ordre partiel $\triangleleft$ sur les partitions de la manière suivante. Soient $\nu = (n_1 \geqslant n_2 \geqslant \cdots \geqslant n_k)$ et $\nu' = (n'_1 \geqslant n'_2 \geqslant \cdots \geqslant n'_{k'})$ deux partitions de n. Quitte à ajouter des zéros, nous pouvons supposer que k et k' sont égaux.

Nous écrirons $\nu' \triangleleft \nu$ (nous dirons alors que la partition ν *domine* la partition ν') si

$$\begin{cases} n'_1 \leqslant n_1 \\ n'_1 + n'_2 \leqslant n_1 + n_2 \\ n'_1 + n'_2 + n'_3 \leqslant n_1 + n_2 + n_3 \\ \vdots \\ n'_1 + n'_2 + \cdots + n'_{k-1} \leqslant n_1 + n_2 + \cdots + n_{k-1}. \end{cases}$$

Diagramme de Young gauche. Soit ν' une partition de n'. Si $D^\nu \supset D^{\nu'}$ nous noterons $D^{\nu \smallsetminus \nu'}$ la différence $D^\nu \smallsetminus D^{\nu'}$; le diagramme $D^{\nu \smallsetminus \nu'}$ est appelé un *diagramme de Young gauche*.

Poids d'un tableau de Young. Nous dirons qu'un tableau T est de *poids* $\mu = (m_1, m_2, \dots, m_l)$ si ses entrées sont constituées de m_1 nombres 1, m_2 nombres $2, \dots,$ m_ℓ nombres ℓ.

Nombres de Kostka. Pour toute partition ν et toute suite $\mu = (m_1, m_2, \dots, m_l)$ d'entiers positifs ou nuls, nous noterons $K_{\nu,\mu}$ le nombre de tableaux de forme ν et de poids μ. De manière équivalente, $K_{\nu,\mu}$ est le nombre de suites de partitions $\nu^{(1)} \subset \nu^{(2)} \subset \cdots \nu^{(l)} = \nu$ telles que le diagramme de Young gauche $\nu^{(i)}/\nu^{(i-1)}$ possède m_i boîtes, avec au plus une boîte dans chaque colonne. Lorsque μ est aussi une partition, le nombre $K_{\nu,\mu}$ est appelé le *nombre de Kostka* associé à la paire de partitions (ν, μ).

Si ν et μ sont deux partitions d'un même entier, on a $K_{\nu,\mu} \neq 0$ si et seulement si $\mu \lhd \nu$.

Partition duale. Nous associons à toute partition $\nu = (n_1 \geqslant n_2 \geqslant \cdots \geqslant n_k)$ de n la partition ν^* de n, dite *partition duale* de ν, définie par
$$\nu^* := (k^{n_k}, (k-1)^{n_{k-1}-n_k}, \dots, (1)^{n_1-n_2}).$$
On a $(\nu^*)^* = \nu$. On vérifie facilement que $\mu \lhd \nu$ si et seulement si $\nu^* \lhd \mu^*$.

Exemple. Les partitions (n) et (1^n) sont duales l'une de l'autre.

Lemme 4.2. *Soient ν et ν' deux partitions de n telles que ν ne domine pas strictement ν', et soient T et T' deux numérotations de formes ν et ν' respectivement.*

Alors,

(a) *ou bien il existe deux entiers distincts apparaissant dans une même ligne de T' et dans une même colonne de T, ou bien $\nu' = \nu$ et il existe $\sigma' \in L(T')$ et $\sigma'' \in C(T)$ telles que $\sigma' \cdot T' = \sigma'' \cdot T$;*

(b) *s'il existe une paire d'entiers figurant dans une même ligne de T' et dans une même colonne de T, alors $b_T \cdot \{T'\} = 0$; dans le cas contraire, on a $b_T \cdot \{T'\} = \pm v_T$.*

Démonstration. Nous allons prouver l'assertion (a) par l'absurde. Supposons que les entrées de la dernière ligne de T' apparaissent dans des colonnes différentes de T. Il existe alors $\sigma''_1 \in C(T)$ telle que ces entrées apparaissent dans la dernière ligne de $\sigma_1'' \cdot T$. Les entrées figurant dans l'avant-dernière ligne de T' apparaissant dans différentes colonnes de T, il en est de même de celles de $\sigma_1'' \cdot T$, il existe donc $\sigma_2'' \in C(\sigma_1'' \cdot T) = C(T)$, qui ne bouge pas les entrées égales à celles de la dernière ligne de T', de sorte que ces entrées apparaissent toutes dans les deux dernières lignes de $\sigma_2'' \cdot \sigma_1'' \cdot T$. Continuant ainsi, nous obtenons $\sigma_1'', \sigma_2'', \ldots, \sigma_m$ dans $C(T)$ telles que les entrées des m dernières lignes de T' figurent dans les m dernières lignes de $\sigma_m'' \cdot \sigma_{m-1}'' \cdots \sigma_1'' \cdot T$. En particulier, puisque T et $\sigma_m'' \cdot \sigma_{m-1}'' \cdots \sigma_1'' \cdot T$ ont la même forme, il en résulte que $\nu_1' + n_2' + \cdots + \nu_m' \leqslant \nu_1 + n_2 + \cdots + \nu_m$. Comme ceci est vrai pour tout m, il en résulte que $\nu' \lhd \nu$.

Puisque nous avons supposé que ν ne domine pas strictement ν', nous obtenons $\nu' = \nu$. Prenant m égal au nombre de lignes de ν, et posant $\sigma'' := \sigma_m'' \cdot \sigma_{m-1}'' \cdots \sigma_1''$, nous voyons que $\sigma'' \cdot T$ et T' ont les mêmes entrées dans chaque ligne. Il existe donc $\sigma' \in L(T')$ telle que $\sigma' \cdot T' = \sigma'' \cdot T$.

Prouvons maintenant l'assertion (b). Supposons qu'il existe une paire d'entiers dans une même ligne de T' et dans une même colonne de T. Soit alors t la transposition qui les permute. On a $b_T \cdot t = -b_T$, puisque t appartient à $C(T)$, mais $t \cdot \{T'\} = \{T'\}$ puisque $t \in L(T')$. Il s'ensuit que

$$b_T \cdot \{T'\} = b_T \cdot (t \cdot \{T'\}) = (b_T \cdot t) \cdot \{T'\} = -b_T \cdot \{T'\},$$

d'où $b_T \cdot \{T'\} = 0$. S'il n'existe pas de telle paire, soient σ' et σ'' comme ci-dessus. Il s'ensuit

$$\begin{aligned} b_T \cdot \{T'\} &= b_T \cdot \{\sigma' \cdot T'\} = b_T \cdot \{\sigma \cdot T\} \\ &= b_T \cdot \sigma'' \cdot \{T\} = \operatorname{sgn}(\sigma'')\, b_T \cdot \{T\} = \operatorname{sgn}(\sigma'') \cdot v_T. \qquad \square \end{aligned}$$

Nous associons à toute partition ν l'entier $z(\nu)$ défini par

$$z(\nu) := \prod_i i^{c_i(\nu)}\, c_i(\nu)! \tag{4.3}$$

où $c_i(\nu)$ est le nombre de fois que l'entier i apparaît dans ν, *i.e.*, $c_i(\nu)$ est égal au nombre d'entiers j tels que $\nu_j = i$.

D'autre part, les classes de conjugaison dans $\mathfrak{S}_n$ sont en bijection avec les partitions de n. La classe de conjugaison $C(\nu)$ correspondant à la partition ν de n est formée des permutations dont la décomposition en cycles est composée de cycle de longueurs $\nu_1, \nu_2, \ldots, \nu_k$. Le nombre d'éléments de $C(\nu)$ est $n!/z(\nu)$ (en effet, le nombre de manières de disposer n entiers en c_i sous-ensemble de i éléments chacun est $n!/\prod(i!)^{c_i} \cdot \prod c_i!$ et choisir un cycle pour une partie de i éléments multiplie par $i!/i$).

Le lemme suivant est alors une conséquence facile des remarques 4.1.

Lemme 4.4. *Pour toute numérotation standard T de ν, on a*

(a) $b_T \cdot M^\nu = b_T \cdot S^\nu = \mathbb{C} \cdot v_T \neq 0$ *;*
(b) $b_T \cdot M^{\nu'} = b_T \cdot S^{\nu'} = 0$ *si* $\nu' > \nu$.

La proposition suivante est une conséquence facile du lemme 4.4.

Proposition 4.5. *Pour toute partition ν de n, S^ν est une représentation irréductible de $\mathfrak{S}_n$. Toute représentation irréductible de $\mathfrak{S}_n$ est isomorphe à exactement l'un des S^ν.*

Lemme 4.6. *Soit $\vartheta\colon M^\nu \to M^{\nu'}$ un homomorphisme de représentations de $\mathfrak{S}_n$. Si S^ν n'est pas contenu dans le noyau de ϑ alors $\nu' \trianglelefteq \nu$.*

Démonstration. Soit T une numérotation de ν. Puisque v_T n'est pas dans le noyau de ϑ, on a $b_T \cdot \vartheta(\{T\}) = \vartheta(v_T) \neq 0$. Il existe donc une numérotation T' de ν' telle que $b_T \cdot \{T'\} \neq 0$. Si $\nu \neq \nu'$ et si ν ne domine pas ν', nous nous trouvons dans le premier cas de l'assertion (a) du lemme 4.2 et cela contredit l'assertion (b) du lemme 4.2. $\square$

La proposition suivante est démontrée dans [Ful97, § 7.2 Cor.]. Nous en verrons une forme plus précise au corollaire 4.26.

Proposition 4.7. *Il existe des entiers positifs ou nuls $k_{\mu,\nu}$ pour $\mu \triangleright \nu$, tels que*

$$M^\nu \simeq S^\nu \oplus \bigoplus_{\mu \triangleright \nu} (S^\mu)^{\oplus k_{\mu,\nu}}.$$

La proposition suivante est démontrée dans [Ful97, § 7.2 Prop. 2].

Proposition 4.8. *Les éléments v_T, lorsque T décrit l'ensemble des tableaux standard sur ν, forment une base de S^ν.*

Corollaire 4.9. *La dimension de S^ν est égale au nombre de tableaux standard de forme ν.*

Opérations sur les partitions. Soit $\nu = (n_1 \geqslant n_2 \geqslant \cdots \geqslant n_k)$ une partition de n, et, pour chaque $j \in \{1, 2, \ldots, k\}$, soit $\nu^{(j)} := (n_1^{(j)} \geqslant n_2^{(j)} \geqslant \cdots \geqslant n_{k_j}^{(j)})$ une partition de l'entier n_j. Quitte à ajouter des zéros, nous pouvons supposer que les k_j sont tous égaux, soit r leur valeur commune. Nous notons alors

$$\nu^{(1)} \cup \nu^{(2)} \cup \cdots \cup \nu^{(k)} \tag{4.10}$$

l'unique partition de l'entier n telle que

$$c_i(\nu^{(1)} \cup \nu^{(2)} \cup \cdots \cup \nu^{(k)}) = c_i(\nu^{(1)}) + c_i(\nu^{(2)}) + \cdots + c_i(\nu^{(k)}), \tag{4.11}$$

pour tout entier $i \geqslant 1$, et

$$\nu^{(1)} + \nu^{(2)} + \cdots + \nu^{(k)} \tag{4.12}$$

la partition de n définie par

$$\begin{aligned}\nu^{(1)} + \nu^{(2)} + \cdots + \nu^{(k)} \ &:= \ (n_1^{(1)} + n_1^{(2)} + \cdots + n_1^{(k)} \\ &\geqslant n_2^{(1)} + n_2^{(2)} + \cdots + n_2^{(k)} \geqslant \cdots \geqslant n_r^{(1)} + n_r^{(2)} + \cdots + n_r^{(k)}).\end{aligned}$$

Pour chaque partition $\nu = (n_1 \geqslant n_2 \geqslant \cdots \geqslant n_k)$ de l'entier n, nous définissons des applications α_ν, β_ν et τ_ν de $\mathcal{P}(n_1) \times \mathcal{P}(n_2) \times \cdots \times \mathcal{P}(n_k)$ dans $\mathcal{P}(n_1 + n_2 + \cdots + n_k)$ par

$$\alpha_\nu(\nu^{(1)}, \nu^{(2)}, \ldots, \nu^{(k)}) \ := \ \nu^{(1)} + \nu^{(2)} + \cdots + \nu^{(k)}, \tag{4.13}$$

$$\beta_\nu(\nu^{(1)}, \nu^{(2)}, \ldots, \nu^{(k)}) \ := \ \nu^{(1)} \cup \nu^{(2)} \cup \cdots \cup \nu^{(k)} \tag{4.14}$$

et

$$\tau_\nu(\nu^{(1)}, \nu^{(2)}, \ldots, \nu^{(k)}) := ((\nu^{(1)})^*, (\nu^{(2)})^*, \ldots, (\nu^{(k)})^*), \qquad \nu^{(j)} \in \mathcal{P}(n_j). \tag{4.15}$$

Exemples

(a) Considérons les partitions $\nu^{(1)} := (2, 1)$ de l'entier $n_1 := 3$ et $\nu^{(2)} := (4, 2, 2, 2, 2, 1)$ de l'entier $n_2 := 13$, donc $\nu := (n_1, n_2)$ est une partition de 16. Nous obtenons

- $\alpha_\nu(\nu^{(1)} + \nu^{(2)}) = (6, 3, 2, 2, 2, 1)$ et donc $\tau_\nu \circ \alpha_\nu(\nu^{(1)}, \nu^{(2)}) = (6, 5, 2, 1, 1, 1)$;

- $(\nu^{(1)})^* = (2,1)$ et $(\nu^{(2)})^* = (6,5,1,1)$, il s'ensuit

$$c_1((\nu^{(1)})^*) = c_2((\nu^{(2)})^*) = 1, \quad c_i((\nu^{(1)})^*) = 0 \quad \text{si } i \neq 1,2,$$

et

$$c_1((\nu^{(2)})^*) = 2, \quad c_5((\nu^{(2)})^*) = c_6((\nu^{(2)})^*)) = 1,$$
$$c_i((\nu^{(2)})^*)) = 0 \quad \text{si } i \neq 1,5,6,$$

d'où

$$c_1(\nu^{(1)} \cup \nu^{(2)}) = 3,$$
$$c_2(\nu^{(1)} \cup \nu^{(2)}) = 1,$$
$$c_5(\nu^{(1)} \cup \nu^{(2)}) = c_6(\nu^{(1)} \cup \nu^{(2)}) = 1,$$
$$c_i(\nu^{(1)} \cup \nu^{(2)}) = 0$$

si $i \neq 1,2,5,6$, et donc

$$\beta_\nu \circ \tau_\nu(\nu^{(1)}, n^{(2)}) = (6,5,2,1,1,1) = \tau_\nu \circ \alpha_\nu(\nu^{(1)}, n^{(2)}).$$

(b) Il est clair que

$$(n_1) + (n_2) + \cdots + (n_k) = (n_1 + n_2 + \cdots + n_k)$$

et

$$(n_1) \cup (n_2) \cup \cdots \cup (n_k) = (n_1, n_2, \ldots, n_k)$$

D'autre part,

$$(1^{n_1}) + (1^{n_2}) + \cdots + (1^{n_k}) = (k^{n_k}, (k-1)^{n_{k-1}-n_k}, \ldots, 1^{n_1-n_2}). \tag{4.16}$$

et

$$(1^{n_1}) \cup (1^{n_2}) \cup \cdots \cup (1^{n_k}) = (1^{n_1+n_2+\cdots+n_k}). \tag{4.17}$$

On remarque sur ces formules que

$$(1^{n_1})^* + (1^{n_2})^* + \cdots + (1^{n_k})^* = (1^{n_1}) \cup (1^{n_2}) \cup \cdots \cup (1^{n_k})^* \tag{4.18}$$

et

$$(n_1)^* \cup (n_2)^* \cup \cdots \cup (n_k)^* = (n_1 + n_2 + \cdots + n_k)^*, \tag{4.19}$$

i.e.,

(4.20)
$$(\alpha_\nu \circ \tau_\nu)((1^{n_1}), (1^{n_2}), \ldots, (1^{n_k})) = (\tau_\nu \circ \beta_\nu)((1^{n_1}), (1^{n_2}), \ldots, (1^{n_k}))$$

et

$$(4.21)\quad (\beta_\nu \circ \tau_\nu)((n_1),(n_2),\dots,(n_k)) = (\tau_\nu \circ \alpha_\nu)((n_1),(n_2),\dots,(n_k)).$$

La proposition suivante est une conséquence immédiate de l'exemple (b) ci-dessus.

Proposition 4.22. *Les applications α_ν, β_ν et τ_ν sont reliées par les formules suivantes :*

$$\tau_\nu \circ \alpha_\nu = \beta_\nu \circ \tau_\nu \quad \textit{et} \quad \alpha_\nu \circ \tau_\nu = \tau_\nu \circ \beta_\nu.$$

Remarque. Les deux égalités de la proposition sont équivalentes, puisque τ_ν est une involution.

Polynômes de Schur et formule de Frobenius. À toute partition ν de n de longueur au plus k est est associé un polynôme symétrique important $s_\nu(x_1, x_2, \dots, x_k)$, appelé le *polynôme de Schur* de ν. Ce polynôme est défini de la manière suivante à l'aide des tableaux. Nous associons à toute numérotation T du diagramme de Young D^ν le monôme, noté x^T, défini comme étant le produit sur les variables x_i correspondants aux entiers i qui figurent dans T, *i.e.,*

$$x^T = \prod_{i=1}^{k} (x_i)^{\text{nombre de fois que } i \text{ apparaît dans } T}.$$

Le polynôme de Schur $s_\nu(x_1, x_2, \dots, x_k)$ est alors la somme

$$s_\nu(x_1, x_2, \dots, x_k) := \sum x^T$$

sur tous les monômes x^T associés aux tableaux de forme ν comprenant les nombres $1, 2, \dots, k$.

Bien que cela ne soit pas évident sur la définition, ces polynômes sont symétriques et forment une base additive de l'anneau des polynômes symétriques.

Exemples. Le diagramme de Young $D^{(n)}$ est composé d'une unique ligne de n boîtes ; le polynôme de Schur $s_{(n)}(x_1, x_2, \dots, x_k)$ est le n-ème *polynôme symétrique complet*, lequel est la somme de tous les monômes distincts de degré n en les k variables $x_1, x_2, \dots, x_k$. Nous le noterons $h_n(x_1, x_2, \dots, x_k)$.

Le diagramme de Young $D^{(1^n)}$ est composé de n lignes d'une boîte chacune ; le polynôme de Schur $s_{(1^n)}(x_1, x_2, \ldots, x_k)$ est le n-ème *polynôme symétrique élémentaire*, lequel est la somme de tous les monômes de la forme $x_{i_1} x_{i_2} \cdots x_{i_n}$ avec $1 \leqslant i_1 < i_2 < \cdots < i_n \leqslant k$. Nous le noterons $e_n(x_1, x_2, \ldots, x_k)$.

Les polynômes $s_\nu(x_1, x_2, \ldots, x_k)$, lorsque ν décrit l'ensemble des partitions de n de longueur au plus k, forment une base (sur $\mathbb{Z}$) de l'espace des polynômes symétriques homogènes de degré n en les variables $x_1, x_2, \ldots, x_k$.

Remarque. Les polynômes

$$\begin{aligned} h_\nu(x_1, x_2, \ldots, x_k) := h_{n_1}&(x_1, x_2, \ldots, x_k) \cdot \\ &\cdot h_{n_2}(x_1, x_2, \ldots, x_k) \cdots h_{n_k}(x_1, x_2, \ldots, x_k), \end{aligned}$$

(resp. les polynômes

$$\begin{aligned} e_\nu(x_1, x_2, \ldots, x_k) := e_{n_1}&(x_1, x_2, \ldots, x_k) \cdot \\ &\cdot e_{n_2}(x_1, x_2, \ldots, x_k) \cdots e_{n_k}(x_1, x_2, \ldots, x_k)) \end{aligned}$$

lorsque ν décrit l'ensemble des partitions de n d'au plus k colonnes forment une base (sur $\mathbb{Z}$) de l'espace des polynômes symétriques homogènes de degré n en les variables $x_1, x_2, \ldots, x_k$.

Nous posons

$$p_r(x_1, x_2, \ldots, x_k) := x_1^r + x_2^r + \cdots + x_k^r,$$

et

$$\begin{aligned} p_\nu(x_1, x_2, \ldots, x_k) := p_{n_1}&(x_1, x_2, \ldots, x_k) \cdot \\ &\cdot p_{n_2}(x_1, x_2, \ldots, x_k) \cdots p_{n_k}(x_1, x_2, \ldots, x_k). \end{aligned}$$

Les polynômes $p_\nu(x_1, x_2, \ldots, x_k)$ sont appelés les *sommes de Newton*. Les polynômes $p_\nu(x_1, x_2, \ldots, x_k)$ forment une base (sur $\mathbb{Q}$) de l'espace des polynômes symétriques homogènes de degré n en les variables $x_1, x_2, \ldots, x_k$.

Les polynômes

$$s_\nu(x_1, x_2, \ldots, x_k), \quad h_\nu(x_1, x_2, \ldots, x_k),$$
$$e_\nu(x_1, x_2, \ldots, x_k), \quad p_\nu(x_1, x_2, \ldots, x_k)$$

vérifient tous la propriété suivante :

$$(*) \qquad p(x_1, x_2, \ldots, x_\ell, 0, 0, \ldots, 0) = p(x_1, x_2, \ldots, x_\ell).$$

Nous appelons *fonction symétrique de degré* n une famille de polynômes symétriques $p(x_1, x_2, \ldots, x_k)$ de degré n, un pour chaque entier k, satisfaisant à l'identité $(*)$ pour tout $\ell < k$. Nous notons Λ_n le $\mathbb{Z}$-module de toutes ces fonctions avec coefficients entiers. Pour toute partition ν de n, nous notons s_ν, h_ν et e_ν et p_ν les fonctions symétriques correspondantes. Les trois premiers de ces ensembles forment des $\mathbb{Z}$-bases de Λ_n, lorsque ν parcourt l'ensemble des partitions de n, alors que le quatrième forme une $\mathbb{Q}$-base de $\Lambda_n \otimes \mathbb{Q}$. Nous notons

$$\Lambda := \bigoplus_{n=0}^{\infty} \Lambda_n$$

l'anneau gradué des fonctions symétriques. L'anneau Λ s'identifie en l'anneau des polynômes en les variables $h_1, h_2, \ldots$, ou en l'anneau des polynômes en les variables $e_1, e_2, \ldots$. On a

$$h_\mu = \sum_\nu K_{\nu,\mu}\, s_\nu, \quad \text{et} \quad e_\mu = \sum_\nu K_{\nu^*,\mu}\, s_\nu = \sum_\nu K_{\nu,\mu}\, s_{\nu^*}.$$

Nous définissons un produit scalaire $\langle\, ,\, \rangle$ sur Λ_n en demandant que les fonctions de Schur s_λ forment une base orthonormale, *i.e.,* que $\langle s_\nu, s_\nu\rangle = 1$ et $\langle s_\nu, s_\mu\rangle = 0$ si $\mu \neq \nu$.

Nous définissons une involution τ sur Λ comme l'homomorphisme additif qui envoie s_ν sur s_{ν^*}. En particulier, on a $\tau(h_n) = e_n$.

La proposition suivante est démontrée dans [Ful97, § 6.2, Cor. 1].

Proposition 4.23

(a) *L'involution τ est un homomorphisme d'anneau et une isométrie.*

(b) *On a $\tau(h_\nu) = e_\nu$ et $\tau(p_\mu) = (-1)^{\Sigma(\mu_i - 1)} p_\mu$.*

Si ν et μ sont des partitions du même entier n, nous définissons des entiers χ_μ^ν par la formule :

$$p_\mu = \sum_\nu \chi_\mu^\nu \, s_\nu.$$

On a $\langle p_\nu, p_\nu \rangle = z(\nu)$ et $\langle p_\nu, p_\mu \rangle = 0$ si $\mu \neq \nu$. Il s'ensuit que

$$s_\nu = \sum_\mu \frac{\chi_\mu^\nu}{z(\mu)} \, p_\mu.$$

Proposition 4.24 **(Formule de Frobenius).** *La valeur du caractère de S^ν sur la classe de conjugaison $C(\mu)$ est l'entier χ_μ^ν.*

L'anneau des représentations et les fonctions symétriques

Soit $\mathfrak{R}_n$ le groupe abélien libre sur les classes d'isomorphisme de représentations irréductibles de $\mathfrak{S}_n$. Une représentation V de $\mathfrak{S}_n$ détermine la classe $[V]$ dans $\mathfrak{R}_n$ définie par

$$[V] = \sum_\nu m_\nu \, [S^\nu],$$

si $V \simeq \bigoplus (S^\nu)^{\oplus m_\nu}$. De manière équivalente, $\mathfrak{R}_n$ est le groupe de Grothendieck de la catégorie des représentations de $\mathfrak{S}_n$, *i.e.*, le groupe abélien libre sur l'ensemble des classes d'isomorphisme de représentations de $\mathfrak{S}_n$, modulo le sous-groupe engendré par les $[V \oplus W] - [V] - [W]$. Nous posons $\mathfrak{R} := \bigoplus \mathfrak{R}_n$, où $\mathfrak{R}_0 := \mathbb{Z}$. Nous définissons un produit $\mathfrak{R}_{n_1} \times \mathfrak{R}_{n_2} \to \mathfrak{R}_{n_1+n_2}$, noté $\times$ par la formule :

$$[V_1] \times [V_2] := \left[\mathrm{Ind}_{\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2}}^{\mathfrak{S}_{n_1+n_2}} (V_1 \otimes_{\mathbb{C}} V_2)\right].$$

Ici le produit tensoriel $V_1 \otimes_{\mathbb{C}} V_2$ est vu comme une représentation du groupe $\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2}$ de la manière évidente : $(\sigma_1 \times \sigma_2) \cdot (v_1 \otimes v_2) := \sigma_1(v_1) \otimes \sigma_2(v_2)$; et $\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2}$ est considéré comme un sous-groupe de $\mathfrak{S}_{n_1+n_2}$ de la manière évidente suivante ; $\mathfrak{S}_{n_1}$ agit sur les n_1 premiers entiers et $\mathfrak{S}_{n_2}$ agit sur les n_2 derniers. La représentation induite est définie par

$$\mathrm{Ind}_{\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2}}^{\mathfrak{S}_{n_1+n_2}} (V_1 \otimes_{\mathbb{C}} V_2) := \mathbb{C}[\mathfrak{S}_{n_1+n_2}] \otimes_{\mathbb{C}[\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2}]} (V_1 \otimes_{\mathbb{C}} V_2).$$

Exemple de représentation induite. Pour toute numérotation T de forme ν, nous avons le sous-groupe $L(T)$ de $\mathfrak{S}_n$. Le fait que M^ν a pour base les éléments de la forme $\sigma \cdot \{T\}$ lorsque σ parcourt les représentations de $\mathfrak{S}_n/L(T)$, signifie que M^ν est isomorphe à la représentation induite

$$\mathrm{Ind}_{L(T)}^{\mathfrak{S}_n}(1) = \mathbb{C}[\mathfrak{S}_n] \otimes_{\mathbb{C}[L(T)]} \mathbb{C}$$

de la représentation triviale de $L(T)$.

Il est facile de vérifier que le produit $\times$ sur $\mathfrak{R}$ est bien défini et qu'il fait de $\mathfrak{R}$ un anneau gradué avec unité, associatif et commutatif.

Nous définissons un produit scalaire symétrique $\langle\,,\,\rangle$ sur $\mathfrak{R}_n$ en demandant que les $[S^\nu]$ en forment une base orthonormale. On montre que

$$\langle [V_1], [V_2] \rangle = \sum_\mu \frac{1}{z(\mu)}\, \chi_{V_1}(C(\mu))\, \chi_{V_2}(C(\mu)),$$

où χ_1 et χ_2 désignent les caractères respectifs de V_1 et V_2.

Nous définissons une involution additive τ sur $\mathfrak{R}_n$ par

$$\tau([V]) := [V \otimes S^{(1^n)}].$$

Puisque les polynômes h_ν forment une base de l'anneau Λ des fonctions symétriques, nous pouvons définir un homomorphisme additif $\varphi\colon \Lambda \to \mathfrak{R}$ par la formule

$$\varphi(h_\nu) := [M^\nu].$$

Le théorème suivant est démontré dans [Ful97, § 7.3, Th. et Prop. 3].

Théorème 4.25

(a) *L'homomorphisme φ est un homomorphisme d'anneaux gradués et est un isomorphisme isométrique de Λ sur $\mathfrak{R}$.*

(b) *On a $\varphi(s_\nu) = [S^\nu]$.*

(c) *L'isomorphisme φ et l'involution τ commutent : $\varphi \circ \tau = \tau \circ \varphi$.*

L'homomorphisme φ nous permet donc de transporter aux représentations les résultats obtenus sur les fonctions symétriques.

***Corollaire 4.26* (règle de Young).** *Pour tout $\nu \in \mathcal{P}(n)$:*

$$M^\nu \simeq S^\nu \oplus \bigoplus_{\mu \rhd \nu} (S^\mu)^{\oplus K_{\mu,\nu}},$$

où $K_{\mu,\nu}$ est le nombre de Kostka.

Nous notons $K = (K_{\mu,\nu})_{\mu,\nu\in\mathcal{P}(n)}$ la matrice à coefficients complexes dont les entrées sont les nombres de Kostka. Nous avons vu que

(a) pour tout $\nu \in \mathcal{P}(n)$ et tout $\mu \in \mathcal{P}(n)$, si $K_{\mu,\nu} \neq 0$, alors $\nu \lhd \mu$;

(b) pour tout $\nu \in \mathcal{P}(n)$, on a $K_{\nu,\nu} = 1$.

Il s'ensuit

$$M^\nu \simeq \bigoplus_{\mu\in\mathcal{P}(n)} (S^\mu)^{\oplus K_{\mu,\nu}}.$$

La matrice K est inversible et nous notons $\widetilde{K} = (\widetilde{K}_{\mu,\nu})_{\mu,\nu\in\mathcal{P}(n)}$ son inverse. La matrice $\widetilde{K}$ possède les propriétés suivantes :

(a) pour tout $\nu \in \mathcal{P}(n)$ et tout $\mu \in \mathcal{P}(n)$, si $\widetilde{K}_{\mu,\nu} \neq 0$, alors $\nu \lhd \mu$;

(b) pour tout $\nu \in \mathcal{P}(n)$, on a $\widetilde{K}_{\nu,\nu} = 1$.

Il résulte de la règle de Young que, pour tout $\nu \in \mathcal{P}(n)$:

$$S^\nu \simeq M^\nu \oplus \bigoplus_{\nu\lhd\mu} (M^\mu)^{\oplus \widetilde{K}_{\mu,\nu}} \simeq \bigoplus_{\mu\in\mathcal{P}(n)} (M^\mu)^{\oplus \widetilde{K}_{\mu,\nu}}. \tag{4.27}$$

Nous associons à tout $(\nu^{(1)}, \nu^{(2)}, \ldots, \nu^{(k)}, \mu) \in \mathcal{P}(n_1) \times \mathcal{P}(n_2) \times \cdots \times \mathcal{P}(n_k) \times \mathcal{P}(n)$, avec $n = n_1 + n_2 + \cdots + n_k$, le nombre complexe $a^\mu_{\nu^{(1)},\nu^{(2)},\ldots,\nu^{(k)}}$ défini par :

$$a^\mu_{\nu^{(1)},\nu^{(2)},\ldots,\nu^{(k)}} := \sum_{\substack{(\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(k)})\in \\ \mathcal{P}(n_1)\times\mathcal{P}(n_2)\times\cdots\times\mathcal{P}(n_k)}} K_{\mu,\lambda^{(1)}\cup\lambda^{(2)}\cup\cdots\cup\lambda^{(k)}} \prod_{j=1}^{k} \widetilde{K}_{\lambda^{(j)},\nu^{(j)}}, \tag{4.28}$$

où $\nu^\cup$ est la partition de n définie en (4.10).

Nous notons $\mathcal{P}^\cup_{\nu^{(1)},\nu^{(2)},\ldots,\nu^{(k)}}$ le sous-ensemble de $\mathcal{P}(n)$ formé des partitions μ qui vérifient les deux propriétés suivantes :

- $\nu^{(1)} \cup \nu^{(2)} \cup \cdots \cup \nu^{(k)} \lhd \mu$,
- $\mu \neq \nu^{(1)} \cup \nu^{(2)} \cup \cdots \cup \nu^{(k)}$;

et $\mathcal{P}^+_{\nu^{(1)},\nu^{(2)},\ldots,\nu^{(k)}}$ le sous-ensemble de $\mathcal{P}(n)$ formé des partitions μ qui vérifient les deux propriétés suivantes :

- $\mu \lhd \nu^{(1)} + \nu^{(2)} + \cdots + \nu^{(k)}$,
- $\mu \neq \nu^{(1)} + \nu^{(2)} + \cdots + \nu^{(k)}$,

où $\nu^{(1)} + \nu^{(2)} + \cdots + \nu^{(k)}$ et $\nu^{(1)} \cup \nu^{(2)} \cup \cdots \cup \nu^{(k)}$ sont les partitions de n définies respectivement en (4.12) et en (4.10). Nous posons

$$\mathcal{P}^{\cup,+}_{\nu^{(1)},\nu^{(2)},\ldots,\nu^{(k)}} := \mathcal{P}^\cup_{\nu^{(1)},\nu^{(2)},\ldots,\nu^{(k)}} \cap \mathcal{P}^+_{\nu^{(1)},\nu^{(2)},\ldots,\nu^{(k)}}.$$

La règle de Young admet alors la généralisation suivante, où l'on induit une représentation irréductible arbitraire d'un sous-groupe de Young alors que pour la règle de Young on induit seulement la représentation triviale.

Théorème 4.29. *Pour tout entier $n \in \mathbb{N}^*$, toute partition $\nu = (n_1 \geqslant n_2 \geqslant \cdots \geqslant n_k)$ de n, et tout k-uplet $(\nu^{(1)}, \nu^{(2)}, \dots, \nu^{(k)}) \in \mathcal{P}(n_1) \times \mathcal{P}(n_2) \times \cdots \times \mathcal{P}(n_k)$, dans le groupe de Grothendieck $\mathfrak{R}_n$,*

$$[S^{\nu^{(1)}}] \times [S^{\nu^{(2)}}] \times \cdots \times [S^{\nu^{(k)}}]$$

est égal à

$$[S^{\nu^{(1)}+\nu^{(2)}+\cdots+\nu^{(k)}}] + [S^{\nu^{(1)}\cup\nu^{(2)}\cup\cdots\cup\nu^{(k)}}] + \sum_{\mu \in \mathcal{P}^{\cup,+}_{\nu^{(1)},\nu^{(2)},\dots,\nu^{(k)}}} a^{\mu}_{\nu^{(1)},\nu^{(2)},\dots,\nu^{(k)}} \, [S^{\mu}].$$

Remarque. Le résultat ci-dessus est nouveau. Des cas particuliers sont démontrés dans [Wal01, VIII.2] et [Aub03, Prop. 3.1]. La preuve donnée ici s'inspire de celle de [Wal01].

Exemple. Supposons $\nu^{(j)} = (n_j)$ pour tout $j \in \{1, 2, \dots, k\}$. Puisque $\widetilde{K}_{\lambda^{(j)},\nu^{(j)}} \neq 0$ implique $\nu^{(j)} \vartriangleleft \lambda^{(j)}$, le seul des termes $\widetilde{K}_{\lambda^{(j)},\nu^{(j)}}$ de $a^{\mu}_{\nu^{(1)},\nu^{(2)},\dots,\nu^{(k)}}$ qui est non nul, est $\widetilde{K}_{\nu^{(j)},\nu^{(j)}}$, qui vaut 1. Comme

$$(n_1) \cup (n_2) \cup \cdots \cup (n_k) = (n_1, n_2, \dots, n_k) = \nu,$$

nous obtenons

$$a^{\mu}_{\nu^{(1)},\nu^{(2)},\dots,\nu^{(k)}} = K_{\mu,\nu}.$$

Nous retrouvons donc la règle de Littlewood-Richardson.

Démonstration. Par définition du produit $\times$ dans $\mathfrak{R}_n$:

$$[S^{\nu^{(1)}}] \times [S^{\nu^{(2)}}] \times \cdots \times [S^{\nu^{(k)}}] = \left[\mathrm{Ind}^{\mathfrak{S}_n}_{\mathfrak{S}_{n_1}\times\mathfrak{S}_{n_2}\times\cdots\times\mathfrak{S}_{n_k}} (S^{\nu^{(1)}} \otimes S^{\nu^{(2)}} \otimes \cdots \otimes S^{\nu^{(k)}})\right].$$

En appliquant (4.27) à chacun des $S^{\nu^{(j)}}$, nous voyons que

$$\left[S^{\nu^{(1)}} \otimes S^{\nu^{(2)}} \otimes \cdots \otimes S^{\nu^{(k)}}\right]$$

est égal à
$$\sum_{\substack{(\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(k)})\in\\ \mathcal{P}(n_1)\times\mathcal{P}(n_2)\times\cdots\times\mathcal{P}(n_k)}} \textstyle\prod_{j=1}^k \widetilde{K}_{\lambda^{(j)},\nu^{(j)}} \left[M^{\lambda^{(1)}}\otimes M^{\lambda^{(2)}}\otimes\cdots\otimes M^{\lambda^{(k)}}\right].$$
Par construction, pour
$$(\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(k)})\in\mathcal{P}(n_1)\times\mathcal{P}(n_2)\times\cdots\times\mathcal{P}(n_k),$$
on a l'égalité
$\mathrm{Ind}_{\mathfrak{S}_{n_1}\times\mathfrak{S}_{n_2}\times\cdots\times\mathfrak{S}_{n_k}}^{\mathfrak{S}_n}(M^{\lambda^{(1)}}\otimes M^{\lambda^{(2)}}\otimes\cdots\otimes M^{\lambda^{(k)}}) = M^{\lambda^{(1)}\cup\lambda^{(2)}\cup\cdots\cup\lambda^{(k)}}$.
Il s'ensuit que
$$\left[\mathrm{Ind}_{\mathfrak{S}_{n_1}\times\mathfrak{S}_{n_2}\times\cdots\times\mathfrak{S}_{n_k}}^{\mathfrak{S}_n}(S^{\nu^{(1)}}\otimes S^{\nu^{(2)}}\otimes\cdots\otimes S^{\nu^{(k)}})\right]$$
est égal à
$$\sum_{\substack{(\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(k)})\in\\ \mathcal{P}(n_1)\times\mathcal{P}(n_2)\times\cdots\times\mathcal{P}(n_k)}} \prod_{j=1}^k \widetilde{K}_{\lambda^{(j)},\nu^{(j)}} \left[M^{\lambda^{(1)}\cup\lambda^{(2)}\cup\cdots\cup\lambda^{(k)}}\right],$$
i.e., (en appliquant la règle de Young au terme $M^{\lambda^{(1)}\cup\lambda^{(2)}\cup\cdots\cup\lambda^{(k)}}$) est égal à
$$\sum_{\mu\in\mathcal{P}(n)} \sum_{\substack{(\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(k)})\in\\ \mathcal{P}(n_1)\times\mathcal{P}(n_2)\times\cdots\times\mathcal{P}(n_k)}} \prod_{j=1}^k \widetilde{K}_{\lambda^{(j)},\nu^{(j)}}\, K_{\mu,\lambda^{(1)}\cup\lambda^{(2)}\cup\cdots\cup\lambda^{(k)}}[S^\mu].$$
En utilisant les propriétés des matrices $\widetilde{K}$ et K citées précédemment, et le fait évident que si $\nu^{(j)}\trianglelefteq\lambda^{(j)}$ pour tout $j\in\{1,2,\ldots,k\}$, alors
$$\nu^{(1)}\cup\nu^{(2)}\cup\cdots\cup\nu^{(k)}\trianglelefteq\lambda^{(1)}\cup\lambda^{(2)}\cup\cdots\cup\lambda^{(k)},$$
avec égalité si et seulement si $\nu^{(j)}=\lambda^{(j)}$ pour tout $j\in\{1,2,\ldots,k\}$, nous obtenons l'égalité
$$\begin{aligned}&[S^{\nu^{(1)}}]\times[S^{\nu^{(2)}}]\times\cdots\times[S^{\nu^{(k)}}]\\ &\qquad= [S^{\nu^{(1)}\cup\nu^{(2)}\cup\cdots\cup\nu^{(k)}}] + \sum_{\mu\in\mathcal{P}^{\cup}_{\nu^{(1)},\nu^{(2)},\ldots,\nu^{(k)}}} a^{\mu}_{\nu^{(1)},\nu^{(2)},\ldots,\nu^{(k)}}[S^\mu].\end{aligned}$$
L'assertion du théorème s'obtient alors « par dualité » en appliquant l'involution τ à l'égalité ci-dessus, en remarquant que τ commute à l'induction (*i.e.,* en utilisant le fait que, de part sa définition, τ est un homomorphisme de l'anneau $\mathfrak{R}_n$) et la proposition 4.22. $\square$

La règle de Littlewood-Richardson

Mot associé à un tableau 4.30. *On lit les entrées d'un tableau T de gauche à droite et de bas en haut. Le mot ainsi obtenu est appelé le mot associé au tableau T.*

Remarque. Le mot permet de retrouver le tableau correspondant : on lit le mot de gauche à droite et l'on coupe dès que l'on rencontre une entrée strictement supérieure à la suivante. Le mot associé au tableau T sera noté $m(T)$.

Exemple. Le mot 5644623551223 correspond au tableau

$$\begin{array}{cccc} 1 & 2 & 2 & 3 \\ 2 & 3 & 5 & 5 \\ & 4 & 4 & 6 \\ & & 5 & 6 \end{array}$$

Un $x_1 x_2 \cdots x_s$ qui, lorsqu'on le lit en partant de la fin jusqu'à une lettre arbitraire x_i, la suite $x_s x_{s-1} \cdots x_{i+1} x_i$ contient au moins autant de 1 que de 2, au moins autant de 2 que de 3, et ainsi de suite, est appelé un *mot de Yamanouchi.*

Exemples. Le mot 2132121 est de Yamanouchi, alors que le mot 1232121 n'est pas de Yamanouchi.

Définition 4.31. *Un tableau gauche T est dit de Littlewood-Richardson si le mot $m(T)$ associé à T est de Yamanouchi.*

Notation 4.32. *Nous notons $c^{\mu}_{\nu^{(1)},\nu^{(2)}}$ le nombre de tableaux gauches de Littlewood-Richardson de forme $\mu/\nu^{(1)}$ et de poids $\nu^{(2)}$.*

La formule

$$s_{\nu^{(1)}} \cdot s_{\nu^{(2)}} = \sum_{\mu \in \mathcal{P}(n)} c^{\mu}_{\nu^{(1)},\nu^{(2)}} \, s_\mu$$

(démontrée par exemple en [Ful97, § 5.2, Cor. 3]) a pour conséquence le résultat suivant.

Corollaire 4.33 **(Règle de Littlewood-Richardson)**

Soient n_1 et n_2 deux entiers strictement positifs. Pour toute paire

$(\nu^{(1)}, \nu^{(2)}) \in \mathcal{P}(n_1) \times \mathcal{P}(n_2)$, *on a*

$$S^{\nu^{(1)}} \times S^{\nu^{(2)}} \simeq \bigoplus_{\mu \in \mathcal{P}(n_1+n_2)} (S^\mu)^{\oplus c^\mu_{\nu^{(1)},\nu^{(2)}}}.$$

Corollaire 4.34. *Pour tout triplet* $(\nu^{(1)}, \nu^{(2)}, \mu) \in \mathcal{P}(n_1) \times \mathcal{P}(n_2) \times \mathcal{P}(n_1+n_2)$, *on a*

$$a^\mu_{\nu^{(1)},\nu^{(2)}} = c^\mu_{\nu^{(1)},\nu^{(2)}}.$$

Références

[Art55a] E. Artin – « The orders of the classical simple groups », *Comm. Pure Appl. Math.* **8** (1955), p. 455–472.

[Art55b] ———, « The orders of the linear groups », *Comm. Pure Appl. Math.* **8** (1955), p. 355–365.

[Art96] ———, *Algèbre géométrique*, Les Grands Classiques Gauthier-Villars, Éditions Jacques Gabay, Paris, 1996, Traduction par M. Lazard de l'édition originale en anglais de 1957. Réédition de l'édition française de 1962.

[ABFS99] M. Aschbacher, H. Bender, W. Feit & R. Solomon – « Michio Suzuki (1926–1998) », *Notices Amer. Math. Soc.* **46** (1999), no. 5, p. 543–551.

[Aub03] A.-M. Aubert – « Character sheaves and generalized Springer correspondence », *Nagoya Math. J.* **170** (2003), p. 47–72.

[AMR96] A.-M. Aubert, J. Michel & R. Rouquier – « Correspondance de Howe pour les groupes réductifs sur les corps finis », *Duke Math. J.* **83** (1996), no. 2, p. 353–397.

[Bur55] W. Burnside – *Theory of groups of finite order*, 2^e éd., Dover Publications, Inc., New York, 1955, 1^{re} éd. en 1911.

[Car56] R. D. Carmichael – *Introduction to the theory of groups of finite order*, Dover Publications, Inc., New York, 1956.

[Car89] R. W. Carter – *Simple groups of Lie type*, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1989.

[Che55] C. Chevalley – « Sur certains groupes simples », *Tohoku Math. J. (2)* **7** (1955), p. 14–66.

[Che97] ———, *The algebraic theory of spinors and Clifford algebras*, Springer-Verlag, Berlin, 1997, Collected works. Vol. 2, Columbia University Press, New York, 1954.

[Con69a] J. H. Conway – « A characterisation of Leech's lattice », *Invent. Math.* **7** (1969), p. 137–142.

[Con69b] ———, « A group of order $8,315,553,613,086,720,000$ », *Bull. London Math. Soc.* **1** (1969), p. 79–88.

[Dic01] L. E. Dickson – « Theory of linear groups in an arbitrary field », *Trans. Amer. Math. Soc.* **2** (1901), no. 4, p. 363–394, Errata : *Ibid.* **3** (1902), no. 4, p. 500.

[Dic02] ———, « A class of groups in an arbitrary realm connected with the configuration of the 27 lines on a cubic surface », *Q. J. Math.* **33** (1902), p. 145–173.

[Dic05] ———, « A new system of simple groups », *Math. Ann.* **60** (1905), p. 137–150.

[Dic07] ———, « A class of groups in an arbitrary realm connected with the configuration of the 27 lines on a cubic surface, II », *Q. J. Math.* **39** (1907), p. 205–209.

[Dic58] ———, *Linear groups : With an exposition of the Galois field theory*, Dover Publications, Inc., New York, 1958, Réédition de l'édition originale de 1901.

[Die71] J. A. Dieudonné – *La géométrie des groupes classiques*, 3[e] éd., Ergeb. Math. Grenzgeb. (3), vol. 5, Springer-Verlag, Berlin-New York, 1971.

[Ema89] M. Emaldi – « Giovanni Frattini 1852–1925 », *Irish Math. Soc. Bull.* (1989), no. 23, p. 57–61.

[Ful97] W. Fulton – *Young tableaux. With applications to representation theory and geometry*, London Math. Soc. Student Texts, vol. 35, Cambridge University Press, Cambridge, 1997.

[FH91] W. Fulton & J. Harris – *Representation theory. A first course*, Graduate Texts in Math., vol. 129, Springer-Verlag, New York, 1991.

[Gér77] P. Gérardin – « Weil representations associated to finite fields », *J. Algebra* **46** (1977), no. 1, p. 54–101.

[Gor68] D. Gorenstein – *Finite groups*, Harper & Row, Publishers, New York-London, 1968.

[How73] R. Howe – « Invariant theory and duality for classical groups over finite fields, with applications to their singular representation theory », Preprint, Yale Univ., 1973.

[Hup67] B. Huppert – *Endliche Gruppen. I*, Grundlehren Math. Wissen., vol. 134, Springer-Verlag, Berlin-New York, 1967.

[Jac75] N. Jacobson – *Lectures in abstract algebra*, Graduate Texts in Math., vol. 30–32, Springer-Verlag, New York-Berlin, 1975.

[Jac85] ———, *Basic algebra. I*, 2[e] éd., W. H. Freeman and Company, New York, 1985.

[Jam78] G. James – *The representation theory of the symmetric groups*, Lect. Notes in Math., vol. 682, Springer, Berlin, 1978.

[JK81] G. James & A. Kerber – *The representation theory of the symmetric group*, Encyclopedia of Mathematics and its applications, vol. 16, Addison-Wesley Publishing Co., Reading, Mass., 1981.

[Jor89] C. Jordan – *Traité des substitutions et des équations algébriques*, Les Grands Classiques Gauthier-Villars, Éditions Jacques Gabay, Sceaux, 1989, Réédition de l'édition originale de 1870.

[KM90] D. Kastler & M. Mebkhout – « Revisiting the Mackey-Stone-von Neumann theorem : the C^*-algebra of a presymplectic space », *Nuclear Phys. B Proc. Suppl.* **18B** (1990), p. 200–211, Recent advances in field theory (Annecy-le-Vieux, 1990).

[Kir74] A. Kirillov – *Éléments de la théorie des représentations*, Éditions Mir, Moscou, 1974.

[Lee67] J. Leech – « Notes on sphere packings », *Canad. J. Math.* **19** (1967), p. 251–267.

[LV80] G. Lion & M. Vergne – *The Weil representation, Maslov index and theta series*, Progress in Math., vol. 6., Birkhäuser, Boston, Mass., 1980.

[Mac89] G. W. Mackey – « Marshall Harvey Stone. 1903–1989 », *Notices Amer. Math. Soc.* **36** (1989), no. 3, p. 221–223.

[Mat61] É. Mathieu – « Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables », *J. Math. Pures Appl.* **6** (1861), p. 241–323.

[Mat73] ———, « Sur la fonction cinq fois transitive de 24 quantités », *J. Math. Pures Appl.* **18** (1873), p. 25–46.

[MVW87] C. Mœglin, M.-F. Vignéras & J.-L. Waldspurger – *Correspondances de Howe sur un corps p-adique*, Lect. Notes in Math., vol. 1291, Springer-Verlag, Berlin, 1987.

[Neu02] M. Neuhauser – « An explicit construction of the metaplectic representation over a finite field », *J. Lie Theory* **12** (2002), no. 1, p. 15–30.

[vN96] J. von Neumann – *Mathematische Grundlagen der Quantenmechanik*, 2e éd., Springer, Berlin, 1996.

[PSA96] J. Pantoja & J. Soto-Andrade – « Représentations de Weil de $\mathrm{SL}_*(2, A)$ et $\mathrm{SL}(n, q)$ », *C. R. Acad. Sci. Paris Sér. I Math.* **323** (1996), no. 10, p. 1109–1112.

[Par89] K. H. Parshall – « Eliakim Hastings Moore and the founding of a mathematical community in America, 1892–1902 », in *A century of mathematics in America, Part II*, Hist. Math., vol. 2, American Mathematical Society, Providence, RI, 1989, p. 155–175.

[Par91] ———, « A study in group theory : Leonard Eugene Dickson's *linear groups* », *Math. Intelligencer* **13** (1991), no. 1, p. 7–11.

[Rot95] J. J. Rotman – *An introduction to the theory of groups*, 4e éd., Graduate Texts in Math., vol. 148, Springer-Verlag, New York, 1995.

[Sag01] B. E. Sagan – *The symmetric group. Representations, combinatorial algorithms, and symmetric functions.*, 2e éd., Graduate Texts in Math., vol. 203, Springer, New York, NY, 2001.

[Sco87] W. R. Scott – *Group theory*, 2e éd., Dover Publications, Inc., New York, 1987.

[Ser78] J.-P. Serre – *Représentations linéaires des groupes finis*, Hermann, Paris, 1978.

[Ser99] ———, « La vie et l'œuvre d'André Weil », *Enseign. Math. (2)* **45** (1999), no. 1-2, p. 5–16.

[Sha62] D. Shale – « Linear symmetries of free boson fields », *Trans. Amer. Math. Soc.* **103** (1962), p. 149–167.

[Suz60] M. Suzuki – « A new type of simple groups of finite order », *Proc. Nat. Acad. Sci. U.S.A.* **46** (1960), p. 868–870.

[Wag78] A. Wagner – « A bibliography of William Burnside (1852–1927) », *Historia Math.* **5** (1978), no. 3, p. 307–312.

[Wal01] J.-L. Waldspurger – *Intégrales orbitales nilpotentes et endoscopie pour les groupes classiques non ramifiés*, Astérisque, vol. 269, Société Mathématique de France, Paris, 2001.

[Wal77] N. R. Wallach – *Symplectic geometry and Fourier analysis*, Lie Groups : History, Frontiers and Applications, vol. V., Math Sci Press, Brookline, Mass., 1977.

[Wei64] A. Weil – « Sur certains groupes d'opérateurs unitaires », *Acta Math.* **111** (1964), p. 143–211.

[Wey39] H. Weyl – *The classical groups. Their invariants and representations*, Princeton University Press, Princeton, NJ, 1939.

[Zel81] A. V. Zelevinsky – *Representations of finite classical groups. A Hopf algebra approach*, Lect. Notes in Math., vol. 869, Springer-Verlag, Berlin-New York, 1981.

Anne-Marie Aubert, Département de Mathématiques et applications (UMR 8553 du CNRS), École Normale Supérieure, 45 rue d'Ulm, 75005 Paris
E-mail : anne-marie.aubert@imj-prg.fr
Url : https://perso.imj-prg.fr/annemarie-aubert/